Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications

Song Guo, *Senior Member, IEEE,* Deze Zeng, *Member, IEEE,* and Yang Xiang, *Senior Member, IEEE*

Abstract—Many services and applications in vehicular ad-hoc networks (VANETs) require preserving and secure data communications. To improve driving safety and comfort, the traffic-related status information will be broadcasted regularly and shared among drivers. Without the security and privacy guarantees, attackers could track their interested vehicles by collecting and analyzing their traffic messages. Hence, anonymous message authentication is an essential requirement of VANETs. On the other hand, when a vehicle is involved in a dispute event of warning message, the certificate authority should be able to recover the real identity of this vehicle. To deal with this issue, we propose a new privacy-preserving authentication protocol with authority traceability using elliptic curve based chameleon hashing. Compared with existing schemes, our approach possesses the following features: (1) mutual and anonymous authentication for both vehicle-to-vehicle and vehicle-to-roadside communications, (2) vehicle unlinkability, (3) authority tracking capability and (4) high computational efficiency. We also demonstrate the merits of our proposed scheme through security analysis and extensive performance evaluation.

Index Terms—security and privacy; ecliptic curve based chameleon hashing; authentication protocol design

1 Introduction

In recent years, the wireless communication technologies have made huge advantages. Based on the tremendous business opportunities, the car manufacturers and telecommunication industries have strained to deploy electronic components with technology that allows vehicles to communicate with each other for the purpose of driving comfort and road safety. For example, a modern car usually has a central computer, an EDR (Event Data Recorder) and a GPS (Global Positioning System) receiver or a navigation system to improve driving experience. A VANET mainly consists of On-Board Units (OBUs) and Roadside Units (RSUs) [1], where OBUs are embedded in vehicles to provide wireless communication capability, while RSUs are located at the critical points on the road to provide wireless interfaces to vehicles within their radio coverage. A bandwidth of 75MHz spectrum in the 5.9GHz that has been allocated to VANETs in the US can support diversified services that range from location dependent service to real-time traffic condition-aware routing optimization and accident prevention [2], [3].

The creation of a VANET not only is significant to traffic management and roadside safety, but also raises formidable research challenges [4]–[6]. Security assurance and privacy preservation are two primary concerns. Without the security and privacy guarantees, adversaries could launch attacks by tracking the location of interested OBUs and abusing their mobility patterns. Therefore, VANET protocols should protect the privacy of the drivers as far as possible and messages from being tampered with by attackers. However, anonymous message authentication is facing a dilemma in VANETs. This is because a well-behaved OBU can achieve a safer and more efficient driving environment by providing its location information to RSUs, while taking the risks that a maliciously-behaved OBU may collect such information to tamper or replay to RSUs. This particularly happens when a driver who is involved in a dispute event of safety message may intend to escape from the investigation and responsibility. Furthermore, conditional privacy preservation must be achieved, i.e., the related private information, such as driver's name, license plate, position, traveling routes and so on, must be protected, while the authorities should be able to reveal sender's real identity when a dispute traffic event happens. That is, the secure protocol should be able to not only protect driver's privacy, but also provide the recovery capability of real identities. Therefore, it is a critical topic to design a privacy protection mechanism to achieve both security and conditional privacy preservation in VANETs.

Since RSUs are located in unattended roadside and can be easily compromised by adversaries, a secure protocol should provide mutual authentication between OBUs and RSUs. Such vehicle-to-RSU (V2R) mutual authentication is neglected by existing protocols [7], [8] for secure vehicular communication. Furthermore, although the comparatively higher computational capability of RSUs makes them the best choice for OBUs' identify verifications [9], their availability cannot always be guaranteed due to the high deployment cost. Therefore, even without RSUs, OBUs shall also be able to mutually

S. Guo and D. Zeng are with the School of Computer Science and Engineering, The University of Aizu, Japan.
E-mail: sguo@u-aizu.ac.jp
Y. Xiang is with the School of Information Technology, Deakin University, Australia.
E-mail: yang.xiang@deakin.edu.au

verify the identity of each other while preserving the privacy of OBUs at the same time. The vehicle-to-vehicle (V2V) authentication is also a major concern for protocol design. Another consideration is efficiency, because the traditional discrete logarithm based method adopted in [7], [8], [10] with high computational cost may not be applicable to VANETs, especially in high traffic conditions.

Those challenges have attracted much research interests and a number of solutions with different design goals have been proposed in the literature. Most solutions (e.g., [10]–[16]) fall in to public key infrastructure (PKI) based approach, which usually uses digital signature technique, e.g., Elliptic Curve (EC) digital signature algorithm and bilinear pairing algorithm, to create anonymous certificates for identity verification. There are also some group-signature based approach (e.g., [7], [8]), where a member of a vehicle group can sign a message on behalf of the group it belongs to, while the identity of the signing member remains hidden within the group. However, to our best knowledge, none of existing solutions can thoroughly achieve all the design goals discussed above. In this paper, to enhance the security and privacy of vehicles by providing both V2R and V2V mutual authentication in an efficient way, we propose a Lightweight Privacy-Preserving (LPP) protocol. To realize time-varying anonymous certificates, we redesign the chameleon signature and integrate it with EC digital signature algorithm. LPP is built upon such EC-based chameleon hash signature, whose unique features not only ensure the privacy and security of VANET communications but also improve the performance of VANET communication due to its low complexity in identity verification. Some key privacy and security properties of the LPP protocol, i.e., anonymity, unlinkability, and replay attack immunity, are analyzed. Furthermore, extensive simulations show that the fast verification of LPP can substantially improve the performance of VANET communication in various scenarios.

The remainder of the paper is organized as follows. Section 3 presents our system model. Section 4 gives an overview of our chameleon hashing based on elliptic curve algorithms. Section 4 describes our Lightweight Privacy-Preserving (LPP) protocol. Sections 6 and 7 provide the security/privacy analysis and performance evaluation of our proposal, respectively. Section 7 gives a brief survey of related work. Finally, Section 8 summarizes our findings.

2 System Model

In this paper, we consider a secure vehicular network model with these types of network entities: the certificate authority (CA), the fixed RSUs at the road side, and the mobile OBUs equipped on the running vehicles. The CA is a registration and certification center for RSUs and OBUs with virtually unlimited computation and storage capability. Only the CA can recover the real identity of an OBU from its certificate. RSUs work as intermediaries between OBU and CA in a semi-trusted way since they are deployed at unattended roadsides. They are responsible for filtering fake messages from malicious or revoked vehicles and reporting OBU's certificate information to CA. OBUs regularly broadcast routine traffic-related status information (e.g., speed, location and acceleration) to help drivers with a better awareness of their driving environment, e.g., enabling early response to an abnormal event.

A secure and lightweight privacy-preserving protocol should meet the following requirements.

1) **V2R Mutual Authentication**: To defend against potential adversary and maliciously-behaved OBUs, it is important to archive mutual authentication between RSU and OBU before they exchange their private or critical information.
2) **V2V Mutual Authentication**: Even in absence of RSUs, OBUs shall also be able to authenticate each other and discover adversary OBUs that may disseminate hazardous messages to ensure the safety of an ad hoc vehicular networks.
3) **Anonymous authentication**: The authentication process should verify the legitimacy of OBUs without revealing their identities.
4) **Unlinkability**: The adversary should not be able to link the packets issued by the same OBU even by eavesdropping transmitted message from the open wireless medium.
5) **Vehicle ID traceability**: A challenging issue of message authentication is to maintain traceability for authority in the presence of the anonymous authentication. Furthermore, the protocol should provide anonymous authentication and unlinkability in traffic message exchanges. Once a dispute event happens, the protocol should be able to recover identities of OBUs according to those anonymous authentication messages.
6) **Efficiency**: The authentication process should be efficient, especially when a large number of vehicles go through an RSU fast, such that the secure link can be established before OBUs leave the communication range.

3 The EC-based Chameleon Hash Signature

Chameleon signature, first introduced in [17], is the basis of our proposed authentication algorithm. A unique characteristic of chameleon signature algorithms is non-interactive. It means that the signature can be generated without interacting with the intended receiver. This way, the performance of authentication can be significantly improved. However, the conventional discrete logarithm based digital chameleon hash signature algorithms (e.g., ID-based chameleon hash [18]) require the same public key issued by the signer for verification. This public key may be peeped by attackers and the unlinkability cannot be guaranteed.

TABLE 1
Notations

G_p	Abelian group
q	a large prime number that can divide $\|G_p\|$
P	a point chosen from G_p
S_b	private key of b, $S_b \in [1, q-1]$
C_b	chameleon of b
CER_b	certificate produced by CA for OBU_b
y_b	public key of b
$h(\cdot)$	a strong one-way hash function
m	an auxiliary parameter
K_{CA}^-	private key of CA
$\alpha_b^{(i)}$	private key of b at session i
$K_{a,b}^{(i)}$	pair-wise key of a and b at session i

To address this issue, we redesign the chameleon hash signature that avoids to use the fixed public keys. The improved version is built upon an Abelian group G_p formed by the points on the elliptic curve as defined in [19], where p is a large prime number. For security consideration, the cardinality of G_p, i.e., $|G_p|$, should be divisible by a large prime number q [19]. A point P chosen from G_p along with the numbers p and q are published by the trust authority as system parameters denoted as (p, P, q). In the following, we present the authentication process between a prover and a verifier using EC-based chameleon hash signature.

Initially, the prover generates its chameleon $C \in G_p$ as $C = S \cdot P$, where S is randomly chosen from [1, q-1] as secret information to the prover. Once the prover needs to be authenticated by the verifier, it generates a new private key α randomly chosen from [1, q-1] and then obtains the corresponding public key y as $y = \alpha \cdot P$. After that, an auxiliary parameter m is found by the collision finding algorithm $CFind(\alpha, nonce, S)$ algorithms as:

$$m = CFind(\alpha, nonce, S) = S - \alpha\gamma, \tag{1}$$

$$\gamma = h(y \oplus nonce), \tag{2}$$

where $nonce$ is the recent challenge provided by the prover and $h(\cdot)$ is a strong one-way hash function, mapping strings of arbitrary length to a number in [1, q-1]. Finally, the prover sends $(C, m, y, nonce)$ to the verifier for authentication.

At the verifier side, the received information $(C, m, y, nonce)$ is used to authenticate the prover by checking if $CH(m, y, nonce)$ is equal to C, where the chameleon hash function $CH(m, y, nonce)$ can be computed as

$$\begin{aligned} CH(m, y, nonce) &= m \cdot P + \gamma \cdot y \\ &= m \cdot P + h(y \oplus nonce) \cdot y. \end{aligned} \tag{3}$$

If $CH(m, y, nonce) = C$ holds, the verifier passes the authentication for the prover. Otherwise, the prover will be considered illegal. For a valid user, the authentication is always successful. It can be confirmed by substituting (1) to (3):

$$\begin{aligned} CH(m, y, nonce) &= m \cdot P + \gamma \cdot y \\ &= (S - \alpha\gamma) \cdot P + \gamma\alpha \cdot P \\ &= S \cdot P = C. \end{aligned} \tag{4}$$

In the proposed signature scheme, the public key y is updated at each authentication session. We shall show in a later section how this EC-based chameleon hash signature can meet all security requirements of VANETs.

4 The Proposed LPP Protocol

In this section, we propose the LPP protocol using EC-based chameleon hash algorithm that exploits dynamic public keys to improve the security and efficiency of VANET communications. It consists of three parts: registration phase, mutual authentication phase and CA tracking phase. In the registration phase, RSUs and OBUs register to CA and pre-load related secret information. Before any traffic exchange between OBU and RSU for V2R communication or between OBUs for V2V communication, two parties should authenticate each other using their pre-loaded information in the mutual authentication phase. Once a disputed event happens, CA executes the CA tracking phase to recover the real identity of the OBU.

4.1 Registration Phase

Both OBUs and RSUs need to be registered with CA. In this registration phase of OBU_b, it generates random number $S_b \in [1, q-1]$ as its secret key and sends its initial chameleon $C_b = S_b \cdot P$ and its real identity ID_b to CA. On receiving the registration request, CA produces a certificate CER_b for OBU_b as

$$CER_b = Sign(C_b, K_{CA}^-) \tag{5}$$

using its private key K_{CA}^- by signing C_b. The information (CER_b, ID_b) is then stored in the database of CA and CER_b will be sent back to OBU_b through a secure channel. Similarly, the certificate of RSU_a is generated as

$$CER_a = Sign(C_a, K_{CA}^-), \tag{6}$$

where $C_a = S_a \cdot P$.

4.2 V2R Mutual Authentication Phase

In this phase, RSU_a initiates the authentication with OBU_b and then they both establish a pair-wise key between each other. The mutual authentication phase is elaborated as follows.

Without loss of generality, we consider a mutual authentication at session i. RSU_a generates a new private key $\alpha_a^{(i)}$ with the corresponding public key $y_a^{(i)} = \alpha_a^{(i)} \cdot P$ that is different from the previous one so as to avoid the linkability problem. Then the auxiliary parameter $m_a^{(i)}$ is updated by $m_a^{(i)} = CFind(\alpha_a^{(i)}, T_a^{(i)}, S_a)$

Algorithm 1 V2R Mutual Authentication between RSA$_a$ and OBU$_b$

RSU$_a$ generates a private key $\alpha_a^{(i)} \in [1, q-1]$ and its corresponding public key $y_a^{(i)} = \alpha_a^{(i)} \cdot P$
RSU$_a$ updates auxiliary parameter $m_a^{(i)}$ as $m_a^{(i)} = CFind(\alpha_a^{(i)}, T_a^{(i)}, S_a)$
RSU$_a$ sends information $\langle CER_a, y_a^{(i)}, m_a^{(i)}, T_a^{(i)} \rangle$ to OBU$_b$
RSU$_a$ receives $\langle CER_a, y_a^{(i)}, m_a^{(i)}, T_a^{(i)} \rangle$ from OBU$_b$
if $Verify(CER_a, K_{CA}^{+}) == CH(m_a^{(i)}, y_a^{(i)}, T_a^{(i)})$ **then**
    OBU$_b$ generates a private key $\alpha_b^{(i)} \in [1, q-1]$ and its corresponding public key $y_b^{(i)} = \alpha_b^{(i)} \cdot P$
    OBU$_b$ updates auxiliary parameter $m_b^{(i)} = CFind(\alpha_b^{(i)}, T_b^{(i)}, S_b)$
    OBU$_b$ generates a pair-wise key as $K_{b,a}^{(i)} = \alpha_b^{(i)} \cdot y_a^{(i)}$
    OBU$_b$ produces encrypted certificate $CER_b' = Encrpt(CER_b \oplus T_b^{(i)}, K_{b,a}^{(i)})$
    OBU$_b$ sends $\langle CER_b', y_b^{(i)}, m_b^{(i)}, T_b^{(i)} \rangle$ to RSU$_a$
end if
RSU$_a$ receives $\langle CER_b', y_b^{(i)}, m_b^{(i)}, T_b^{(i)} \rangle$ from OBU$_b$
RSU$_a$ generates a pair-wise key as $K_{b,a}^{(i)} = \alpha_b^{(i)} \cdot y_a^{(i)}$
RSU$_a$ produces encrypted certificate $CER_b' = Encrpt(CER_b \oplus T_b^{(i)}, K_{b,a}^{(i)})$
if $Verify(CER_b, K_{CA}^{+}) == CH(m_b^{(i)}, y_b^{(i)}, T_b^{(i)})$ **then**
    Mutual authentication completes
end if

where $T_a^{(i)}$ is the current time. Finally, the information $\langle CER_a, m_a^{(i)}, y_a^{(i)}, T_a^{(i)} \rangle$ is sent to OBU$_b$ for verification.

Upon receiving this information, OBU$_b$ uses the public key K_{CA}^{+} of CA to verify the legitimacy of RSU$_a$ by checking:

$$Verify(CER_a, K_{CA}^{+}) = CH(m_a^{(i)}, y_a^{(i)}, T_a^{(i)}). \quad (7)$$

If RSU$_a$ passes the verification, i.e., the above equation holds, a pair-wise $K_{b,a}^{(i)}$ is generated as

$$K_{b,a}^{(i)} = \alpha_b^{(i)} \cdot y_a^{(i)}. \quad (8)$$

To achieve mutual authentication, OBU$_b$ should be also verified by RSU$_a$ following a similar process. The only concern is that the certificate CER_b of OBU$_b$ cannot be sent to RSU$_a$ directly, because each certification is unique and can be used for tracking by adversaries. For this reason, certificate CER_b along with the current time $T_b^{(i)}$ is encrypted by $K_{b,a}^{(i)}$ as

$$CER_b' = Encrpt(CER_b \oplus T_b^{(i)}, K_{b,a}^{(i)}) \quad (9)$$

that guarantees unlinkability of OBU$_b$. Finally, the information $\langle CER_b', m_b^{(i)}, y_b^{(i)}, T_b^{(i)} \rangle$ is sent to RSU$_a$ to complete the mutual authentication.

Using the received information, RSU$_a$ also obtains the same pair-wise key $K_{a,b}^{(i)} = \alpha_a^{(i)} \cdot y_b^{(i)}$ because

$$\begin{aligned} K_{a,b}^{(i)} &= \alpha_a^{(i)} \cdot y_b^{(i)} = \alpha_a^{(i)} \cdot (\alpha_b^{(i)} \cdot P) = \alpha_b^{(i)} \cdot (\alpha_a^{(i)} \cdot P) \\ &= \alpha_b^{(i)} \cdot y_a^{(i)} = K_{b,a}^{(i)}. \end{aligned} \quad (10)$$

Therefore, certification CER_b can be recovered by decrypting CER_b' using pair-wise key $K_{a,b}^{(i)}$, i.e.,

$$CER_b = Decrpt(CER_b', K_{a,b}^{(i)}) \oplus T_b^{(i)}. \quad (11)$$

Note that the freshness of $T_b^{(i)}$ should be examined. Moreover, RSU$_a$ needs to check if CER_b is in the revocation list that is retrieved from CA. If in the list, RSU$_a$ terminates the mutual authentication session immediately. Otherwise, the legitimacy of OBU$_b$ can be verified by checking if

$$Verify(CER_b, K_{CA}^{+}) = CH(m_b^{(i)}, y_b^{(i)}, T_b^{(i)}) \quad (12)$$

holds. After that, the mutual authentication process completes. A brief protocol description of mutual authenticationo process between RSA$_a$ and OBU$_b$ is summarized in Algorithm 1.

4.3 V2V Mutual Authentication Phase

In V2R authentication phase, since no privacy issue is involved for RSUs, their original certificates are sent out directly for the authentication purpose. A major difference in V2V authentication phase is that at each authentication session, the certificate of each party must be encrypted with some variance such that the resulting certificate alters each time and the original certificate can be recovered by a legal receiver. In order to achieve this goal, the V2V mutual authentication phase consists of (1) private key exchange for pairwise key generation and (2) encrypted certification exchange and verification.

We consider a mutual authentication between OBU$_a$ and OBU$_b$ at session i. At the beginning of the session, an updated private key is generated at each side and the corresponding public key included in their periodical beacon messages. After the key exchange, each party calculates their pair-wise key independently such that $K_{a,b}^{(i)} = \alpha_a^{(i)} \cdot y_b^{(i)} = \alpha_b^{(i)} \cdot y_a^{(i)} = K_{b,a}^{(i)}$. At each side, e.g., OBU$_a$, the information $(K_{a,b}^{(i)}, y_b^{(i)})$ for session i is maintained in a pairwise key table at OBU$_a$. Then the pair-wise key is used to produce encrypted certificates $CER_a' = Encrpt(CER_a \oplus T_a^{(i)}, K_{a,b}^{(i)})$ and $CER_b' = Encrpt(CER_b \oplus T_b^{(i)}, K_{b,a}^{(i)})$ at OBU$_a$ and OBU$_b$, respectively.

Another round of message exchange is required by passing the encrypted certificate as well as other information for verification to each other. For example, after receiving $\langle CER_b', y_b^{(i)}, m_b^{(i)}, T_b^{(i)} \rangle$, OBU$_a$ first looks up its pairwise key table for the entry relating to $y_b^{(i)}$ and the corresponding pairwise key $K_{a,b}^{(i)}$ is then used to recover the original certificate CER_b. The remaining verification process for each OBU is then conducted in a similar manner as described in the V2R case.

4.4 CA Tracking Phase

The CA Tracking phase is launched only when dealing with a dispute event. Once the real ID of an OBU needs to be recovered, its CER will be reported to CA. Since each CER is unique, CA can lookup its database to find the identity of corresponding to OBU.

5 Security Analysis

In this section, we analyze some security and privacy issues of our proposal protocol.

5.1 Breaking EC-based Chameleon Hash Function

In the proposed mutual authentication scheme, verification is achieved by the EC-based chameleon hash function that becomes the major breaking target by adversaries. Our theoretical analysis shows that it is as hard as to solve the ECDLP (elliptic curve discrete logarithm problem), which is to determine the integer α such that $\alpha \cdot P = Q$, given $P, Q \in G_p$. It has been proven that ECDLP is NP-complete [19].

By examining authentication messages delivered by OBUs and RSUs in our proposed protocol, we notice that all information included in the messages updates from session to session except the certification of the same RSU. Therefore, the only way to break the EC-based chameleon hash function is to analyze a collection (e.g., k messages) of information sent by a same RSU (e.g., RSU$_x$): $\langle CER_x, m_x^{(i)}, y_x^{(i)}, T_x^{(i)} \rangle, 1 \leq i \leq k$. Based on the definition of the collision finding function, the adversary can establish a linear equation system as follows:

$$\begin{aligned} m_x^{(1)} + \gamma_x^{(1)} \cdot \alpha_x^{(1)} &= m_x^{(2)} + \gamma_x^{(2)} \cdot \alpha_x^{(2)} \\ &= \cdots \\ &= m_x^{(k)} + \gamma_x^{(k)} \cdot \alpha_x^{(k)}, \end{aligned} \tag{13}$$

where $\gamma_x^{(i)} = h(y_x^{(i)} \oplus T_x^{(i)})$ and $m_x^{(i)}$ are known but $\alpha_x^{(i)}$ is variable, $1 \leq i \leq k$. Note that this linear system has k variables but only $k-1$ equations. In other words, at least one variable, e.g., $\alpha_x^{(i)}$, must be conjectured such that $\alpha_x^{(i)} \cdot P = y_x^{(i)}$, where P and $y_x^{(i)}$ are known points on G_p. Therefore, to forge a legitimate EC-based chameleon hash algorithm is equivalent to solve the ECDLP.

5.2 Anonymity and Unlinkability

Our protocol achieves anonymity and unlinkability to the packet tracing attack due to the following properties. (1) The information sent by any OBU (e.g., OBU$_x$): $\langle CER'_x, y_x^{(i)}, T_x^{(i)} \rangle$ is not fixed in different sessions. They cannot be used for tracking by eavesdroppers. (2) The certificate-related information CER'_x is encrypted by a pair-wise key such that the real certificate CER_x cannot be extracted for tracking as well. (3) The pair-wise key is also updated in every session.

5.3 Replay Attack

Our proposed protocol can defend against the replay attack and thus achieves data freshness. The information in any open authentication message $\langle CER_x, m_x^{(i)}, y_x^{(i)}, T_x^{(i)} \rangle$ issued by RSU$_x$ is all linked together, making impersonation on replay attack impossible. Once any value in the open message is modified, the authentication will definitely fail because

$$\begin{aligned} CH(m_x^{(i)}, y_x^{(i)}, T_x^{(i)}) &\neq CH(m_x^{(i')}, y_x^{(i)}, T_x^{(i)}) \\ &\neq CH(m_x^{(i)}, y_x^{(i')}, T_x^{(i)}) \\ &\neq CH(m_x^{(i)}, y_x^{(i)}, T_x^{(i')}). \end{aligned} \tag{14}$$

Similarly, any open authentication message $\langle CER'_x, m_x^{(i)}, y_x^{(i)}, T_x^{(i)} \rangle$ issued by OBU$_x$ cannot be impersonated by replay attack as well.

6 Performance Evaluation

In this section, we use simulations to evaluate the performance of LPP by comparing with the performance of ECPP [10] in different communication scenarios. To the best of our knowledge, ECPP is the protocol that supports both V2R and V2V authentication with the lowest complexity for vehicular communications that is available in the literature. Specially, to show the advantage of the proposed EC based chameleon algorithm, two LPP variants, conventional chameleon using bilinear pairing based (Bi-LPP) and our proposed EC based (EC-LPP) are considered.

6.1 Simulation Setup

We adopt the popular network simulator ns-2.34 [20] in our experiments. The communication between OBUs and RSUs is defined by IEEE 802.11p, which is an approved amendment to the IEEE 802.11 standard with the goal of supporting Dedicated Short-Range Communication (DSRC) [2] in vehicular environments. In addition, we make use of the trace generator VanetMobiSim [21] to generate realistic vehicular mobility traces for both city scenario and highway scenario. For the city scenario, we import a map from the US Census Bureau TIGER/Line database [22] as shown in Fig. 1, which corresponds to Thomas Circle Park area of Washington DC. For the highway scenario, we consider a straight bidirectional eight-lane road. Some important simulation settings are summarized in Table 2. We evaluate these two protocols under various vehicular densities.

We augment ns2 with RSU and OBU agents that accept the authentication time as parameter to simulate their behaviors. The computational cost of ECPP is dominated by scalar multiplication and pairing operation [10]. The dominant factors of EC-LPP are four scalar multiplications and one RSA verification while Bi-LPP requires two bilinear pairing, one scalar multiplication and one RSA verification. Therefore, we first survey the computation costs of those primitive cryptography operations, which

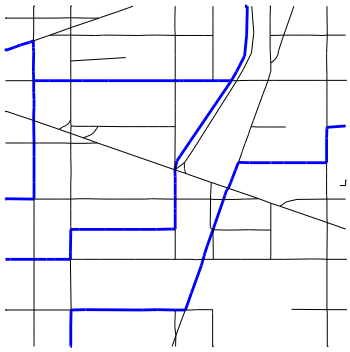


Fig. 1. Random graph-based vehicular with city scenario

TABLE 2
Simulation configuration

IEEE 802.11p settings	
Propagation model	Two Way Ground
Frequency	5.9GHz
Communication range	200m
Data rate	27 Mb/s
City/Highway settings	
City simulation area	$1000m \times 1000m$
High way simulation area	$2500 \times 30m$
Speed of city simulation	25 to 85 km/h
Speed of highway simulation	80 to 145 km/h

are obtained on an Intel Pentium IV 3.0 GHz processor [23], [24] as shown in Table 3. Based on these experimental results and using the same approach adopted in [10], we further analyze the mutual authentication time of EC-LPP, Bi-LPP and ECPP, as given in Table 4. We observe that the complexity is significantly reduced by EC-LPP because it avoids the most expensive operation of pairing in both Bi-LPP and ECPP.

Then we study three representative vehicular communication scenarios to investigate how the authentication time cost shown in Table 4 affects the overall network performance.

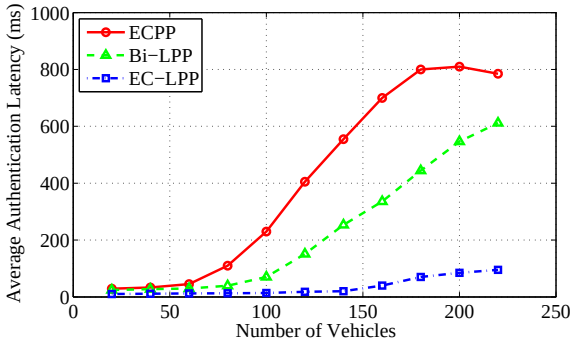
Scenario 1: In this scenario, only single-session V2R mutual authentication process will be conducted when an OBU passes by an RSU. This set of experiment evaluates mutual authentication delay and successful authentication ratio by different protocols.

Scenario 2: We extend Scenario 1 into multi-session case, where an OBU continuously conducts "request-and-reply" interactive communications in certain rate with the corresponding RSU until driving out of its communication range. A reply message will be generated at an RSU as soon as a request is received and verified. A new request will not be issued until a prior reply is received. Notice that in order to guarantee the privacy of all vehicles, they never use their real identities to communicate. Time-varying certificates are adopted for identity verification.

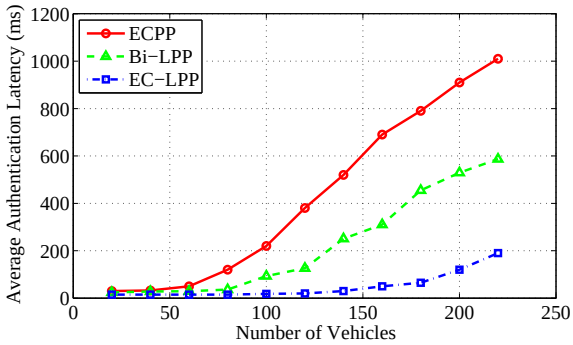
Scenario 3: Besides the above two V2R scenarios, we also consider a V2V scenario. In particular, we study a privacy-preserving secure flooding scenario where some messages (e.g., cooperative collision warning, congested

TABLE 3
Cryptographic Operations' Computation Cost

Symbol	Execution Time	Descriptions
T_{sm}	1.52ms	Scalar multiplication calculating $k \cdot P$
T_{pair}	4.5ms	The time for pairing operation
T_{RV}	0.205ms	RSA verification



(a) In City Scenario



(b) In Highway Scenario

Fig. 2. Average Authentication Latency versus Vehicular Density

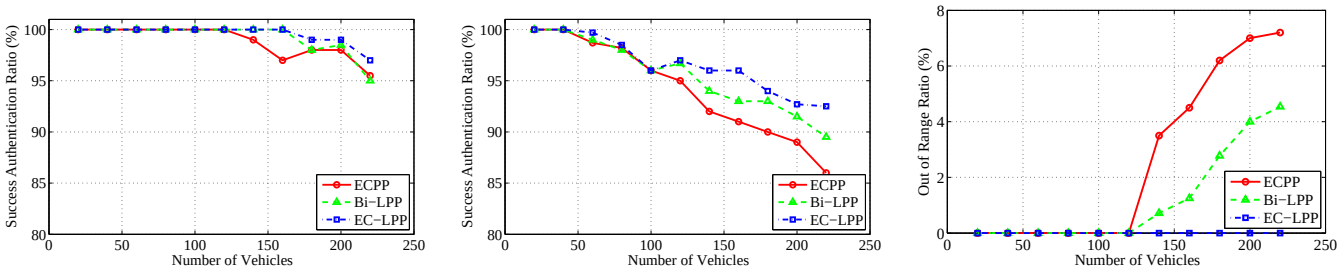
road notifications, etc.) generated at some vehicles can flood to other vehicles nearby. Flooding plays an important role in VANET and has drawn lots of research interests [15], [25], [26]. In order to prevent flooding fake or even hazardous messages from malicious senders, the authenticity of both generator and forwarder shall be verified before further forwarding those messages. Both ECPP and LPP algorithms are able to tackle this issue.

6.2 Single-Session V2R Mutual Authentication

We first investigate how LPP and ECPP perform in realistic scenarios in terms of average authentication latency (AAL). Simulation results in both city and highway scenarios under different vehicular densities are presented in Fig. 2(a) and 2(b), respectively. We observe that the authentication time cost, given in Table 4, has a strong impact on AAL. The AAL achieved by EC-LPP is much lower than Bi-LPP and ECPP in both scenarios due to its light-weight scheme. For example, when there are 100 vehicles in a highway scenario, EC-LPP can achieve an average authentication latency as low as only

TABLE 4
Comparison of Authentication Time Cost

	ECPP	Bi-LPP	EC-LPP
RSU	$T_{sm} + 3T_{pair} = 15.02ms$	$2T_{pair} + T_{sm} + T_{RV} = 10.725ms$	$4T_{sm} + T_{RV} = 6.285ms$
OBU	$4T_{sm} + T_{pair} = 10.58ms$	$2T_{pair} + T_{sm} + T_{RV} = 10.725ms$	$4T_{sm} + T_{RV} = 6.285ms$



(a) SAR in City Scenario (b) SAR in Highway Scenario (c) Out of Range Ratio in High Way Scenario

Fig. 3. Successful Authentication Ratio and Out-of-Range Ratio

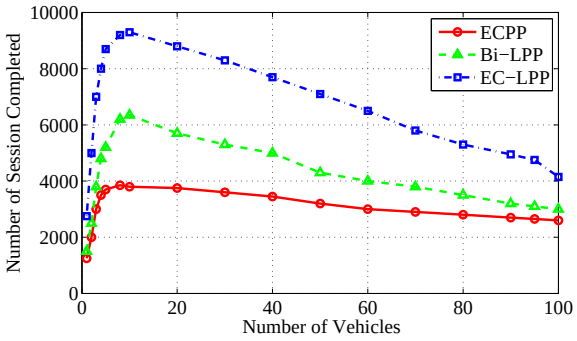
12.86 ms, compared to 70.33ms and 232.13 ms of Bi-LPP and ECPP, respectively. Such advantage becomes more significant with further increase of the vehicle density. One may also notice that the performance of EC-LPP in both scenarios almost keeps constant when the vehicle density is from 20 to 140. Similar observation can be found in ECPP but only from 20 to 50. A constant AAL indicates that no queueing delay is incurred. When the vehicle density exceeds some threshold, AAL increases rapidly because of the service capacity of RSUs, i.e., the number of vehicles that can be verified in a time unit, is reached. Low authentication complexity of EC-LPP implies lower queuing delay, and thus enlarges the service capacity.

Another performance concern is successful authentication ratio (SAR), which is the ratio of vehicles that can be successfully verified. This performance metric relates to both channel quality and authentication latency. The channel quality determines the probability that authentication packets can be successfully received, while longer authentication latency may lead to the abortion of the authentication session because of OBUs running out of the communication range. The results of SAR under various vehicle densities in both city and highway scenarios are shown in Fig. 3. When the speed of a vehicle is not high enough to make it out of the communication range within the authentication latency, the channel quality is the dominant factor (i.e., in the city). As shown in Fig. 3(a), SAR keeps as high as 100% until the vehicle density increases to a certain value (e.g., 160 in EC-LPP). After that, it starts decreasing because higher vehicle density introduces more channel competitions, which lead to severer packet loss. In the city scenario, almost no vehicles go out of the communication range of RSUs on any algorithm. The results of the out-of-range ratio in city scenario are thus omitted. However, the out-of-range cases in ECPP and Bi-LPP appear as shown in Fig. 3(c), when there are more than 120 vehicles in the highway scenario. As witnessed in Fig. 2(b), higher vehicle density results in longer AAL, which further makes more OBUs go out of the communication range of their RSUs before an authentication process finishes. Therefore, ECPP suffers lower SAR in the highway scenario, especially when the vehicle density exceeds 100. Another important fact we notice is that no out-of-range cases happen and the unsuccessful authentication is only introduced by the poor channel condition if EC-LPP is applied.

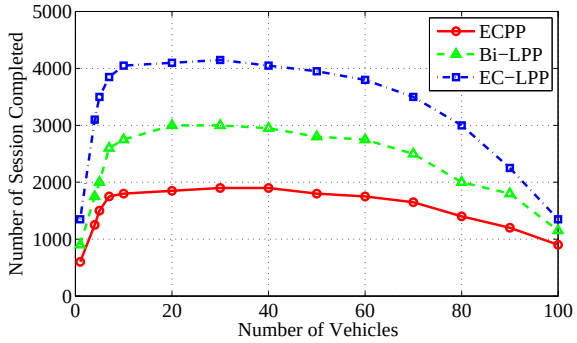
6.3 Multi-Session V2R Mutual Authentication

In this extended scenario, we are most interested in the number of continuous sessions that can be completed within the contact duration between an OBU and an RSU. The number of completed sessions is affected by at least two factors. One is the identity verification speed on both OBU and RSU. A new session can be initiated quicker if the identity of counterpart can be verified faster. Another major factor is the vehicular density (i.e., the number of vehicles associated with an RSU in a time unit). In realistic vehicular deployment, both RSUs and communication channels are regarded as shared scarce resources. The more competitors (i.e., OBUs on vehicles), the less resource an OBU can be allocated. Even worse, more competitions may incur negative side effects, e.g., channel collisions. We evaluate the performance of both ECPP and LPP in terms of total completed sessions per minute under different vehicular densities. The simulation results are shown in Fig. 4.

An obvious performance advantage of EC-LPP over Bi-LPP and ECPP is observed in both scenarios from Fig. 4, where EC-LPP can handle roughly two times number of sessions of ECPP. For example, when there are 20 vehicles associated with the RSU in the city scenario, total 7200 sessions are completed by EC-LPP while only 3000 sessions by ECPP in a minute. This is because

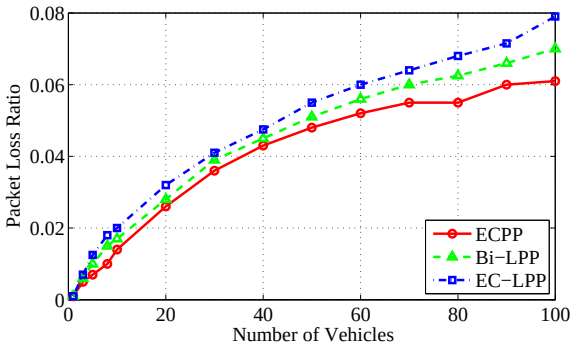


(a) In City Scenario

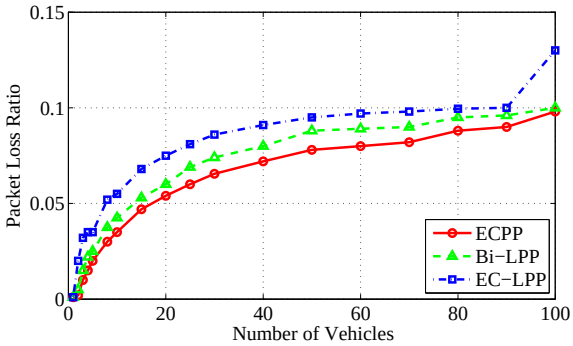


(b) In Highway Scenario

Fig. 4. Number of Completed Sessions versus Vehicular Density



(a) In City Scenario



(b) In Highway Scenario

Fig. 5. Packet Loss Ratio versus Vehicular Density

each session requires two verification processes: one at RSU and the other at the corresponding OBU, and the verification can be done much faster by EC-LPP than ECPP on both ends. Another interesting fact observed from Fig. 4 is that the number of completed sessions first shows as an increasing function and later on becomes a decreasing function of the vehicular density. When the vehicular density is low, the processing capacity of RSU is under-exploited and therefore the completed sessions increase with the number of vehicles. However, after further increasing vehicular density, many communication sessions would fail due to more channel collisions. This conjecture is validated by Fig. 5, which shows the packet loss ratio observed in the simulations as an increasing function of vehicular density for both city and highway settings. Moreover, the packet loss ratio experienced by EC-LPP is a little higher than ECPP. This is because a session can be completed faster using EC-LPP and more traffic (i.e., authentication sessions) has been generated, leading to more collisions.

6.4 V2V Mutual Authentication in Flooding

In the last set of experiments, we next study how these two protocols perform in flooding communication scenario when V2V verification is incorporated. Their performance is evaluated on the *reception delay* of a vehicle, which is defined as the duration between the time when a message is generated at the source and the time when the message is received by this vehicle. We conduct two sets of simulations with different message generation rates, in which 10 vehicles are randomly selected from 400 vehicles to generate messages following a Poisson process. The rates of 3 message per second and 10 messages per second are used to represent the cases of low traffic density and high traffic density, respectively. The experimental results of reception delay in Cumulative Density Function (CDF) are presented in Fig. 6. A major observation is that the reception delay spans a large range. For example, the reception delay by ECPP in high traffic density case may be as low as 0.03 second and as high as 20 seconds. We attribute it to the fact that the distance of vehicle from the message source varies and the message must be transmitted and authenticated hop by hop. Again, EC-LPP exhibits much lower reception delay than both Bi-LPP and ECPP because of its shorter processing (e.g., verification) time at each hop. Moreover, we notice that this delay is also affected by the number of flooding messages accumulated in a forwarder as it determines the queueing delay. This explains why much longer reception delays are experienced in high traffic density case as shown in Fig. 6(b).

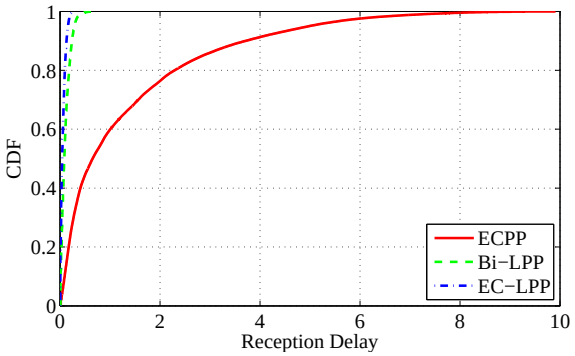
7 Related Work

In this section, we briefly survey the VANET protocols that also cope with conditional privacy preservation in the literature. A number of recent results have addressed VANET authentication and anonymity issues [27]. They

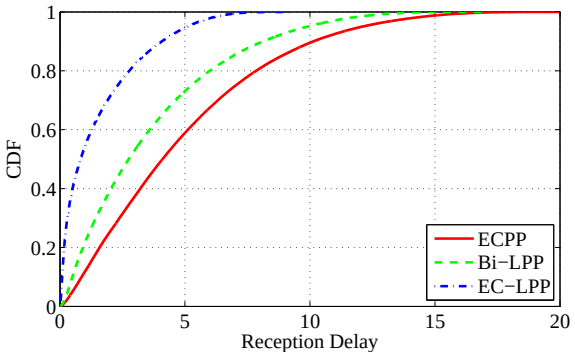
fall into the following two categories, public key based digital signatures and group signature based security schemes.

7.1 Public Key based Digital Signatures

To achieve both message authentication and anonymity, Raya et al. [11] propose a scheme, in which each OBU stores a set of anonymous public/private keys to sign traffic messages so as to avoid being traced by changing private keys periodically. This method allows anonymous message authentication and conditional privacy preservation, but brings the following disadvantages. First, each OBU needs to store a large number of anonymous pair-wise keys. Second, the authority has a high search time on looking up the long revocation list, which is a list of certificates that have been evacuated by certificate authorities, for any dispute certificate. Third, when some OBUs' anonymous keys are revoked, it takes a long time to update the certificate revocation list. To achieve conditional privacy preservation with lower overhead, Lu et al. [10] propose the ECPP protocol based on bilinear pairing [28] algorithm. It provides mutual authentication between RSUs and OBUs, and allows RSUs issuing a short-term certificate with a temporary public/private keys for each valid OBU. Once an RSU receives a short-term certificate, it omits to check the revocation list to achieve a fast hand-over. However, the results of performance evaluation show that the capability of RSUs in ECPP is restricted by the heavy authentication process. To reduce the security overhead of traditional PKI-based security schemes, Zhang et al. [9], [29] introduce an RSU-aided message authentication scheme RAISE. With RAISE, RSUs are responsible for verifying the authenticity of messages sent by vehicles and notifying the authentication results back to all associated vehicles. In addition, they also propose a cooperative message authentication scheme named COMET to work as a supplementary scheme of RAISE in case of the absence of an RSU. However, for traceability, RSU needs to maintain a trace evidence table, which would become huge. Even worse, when there is no cooperation opportunity (i.e., only few vehicles), mutual authentication becomes a complicated task. Later on, Lu et al. [12] propose VANET-based Smart PARKing (SPARK) scheme using bilinear pairing technique to provide drivers with convenient parking services in large parking lots. In SPARK, pseudo-ID is used and a scheme with conditional privacy preservation is also presented. However, it has been shown that bilinear pairings operations are expensive in terms of computational complexity [30]. Furthermore, SPARK fails to provide V2R mutual authentication such that the compromise of the RSU in a parking lot may result in serious consequences. Recently, Shen et al. [16] propose a lightweight protocol using elliptic curve cryptography, but V2V authentication is not addressed. Huang et al. [31] introduce an anonymous batch authentication and



(a) Low traffic density



(b) High traffic density

Fig. 6. The CDFs of Reception Delay

key agreement (ABAKA) scheme, in which an RSU can simultaneously authenticate multiple requests and establish different session keys with vehicles. However, ABAKA suffers serious tracability problem. Especially when there are many adversary requests, it is quite difficult for ABAKA to detect such requests. In addition, ABAKA does not provide V2V mutual authentication such that the failure or compromise of an RSU would make the whole system collapse.

7.2 Group-signature Approaches

Group signature concept, first introduced by Chaum and Van Heyst [32], is a kind of a group-oriented signature with one public key corresponding to multiple private keys held by each group member. The group signature scheme is a method that a group member is allowed to anonymously sign a message on behalf of the group and any one can verify a group signature using a group public key. The important properties of group signature enable group members concealing their identities in the group when OBUs sign a traffic message. Lin et al. [7] propose the GSIS protocol based on the group signature technique. Another group signature based protocol TACKing is proposed in [8]. Compared with GSIS, TACKing provides fast handover that allows OBUs to regularly update their public/private keys. While both GSIS and TACKing do not need to maintain a large number of anonymous keys, they still incur significantly high computational cost. For example, the computational cost

of GSIS for safety message verification grows linearly with the number of revoked OBUs in the revocation list. Even worse, both GSIS and TACKing provide one-way authentication only from RSUs to OBUs. Recently, to void using the certificate revocation list, Jiang et al. [33] propose an anonymized batch authentication based conditional privacy scheme in VANETs but they do not discuss how to achieve mutual authentication between OBUs either.

8 Conclusion

In this paper, we present a novel LPP protocol for VANETs. Through theoretical analysis, we show that LPP satisfies many desired properties for secure and privacy-preserving vehicular communications. We also demonstrate high efficiency of the proposed protocol in a number of representative vehicular communication scenarios by extensive ns2-based simulation. Compared to existing schemes, our proposed protocol can achieve mutual authentication for both V2R and V2V traffics with much lower computational cost, and hence is highly suitable in a realistic vehicular environment.

References

[1] Y. Peng, Z. Abichar, and J. Chang, "Roadside-Aided Routing (RAR) in Vehicular Networks," in *Proceeding of International Conference on Communications (ICC)*, vol. 8. IEEE, Jun. 2006, pp. 3602–3607.

[2] "Dedicated Short Range Communications (DSRC)." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

[3] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments," in *Proceeding of Vehicular Technology Conference (VTC-Spring)*. IEEE, May 2008, pp. 2036 –2040.

[4] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, Jun. 2007.

[5] H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[6] W. Chen, R. K. Guha, T. J. Kwon, J. Lee, and Y.-Y. Hsu, "A survey and challenges in routing and data dissemination in vehicular ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 11, no. 7, pp. 787–795, 2011.

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

[8] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," in *Proceeding of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Jun. 2009, pp. 1–9.

[9] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks," in *Proceeding of International Conference on Communications (ICC)*. IEEE, May 2008, pp. 1451–1457.

[10] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," in *Proceeding of the 27th Conference on Computer Communications (INFOCOM)*. IEEE, Apr. 2008, pp. 1229 –1237.

[11] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, pp. 39–68, January 2007.

[12] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET-Based Smart Parking Scheme for Large Parking Lots," in *Proceeding of the 29th International Conference on Computer Communications (INFOCOM)*. IEEE, Apr. 2009, pp. 1413–1421.

[13] J.-Y. Kim, H.-K. Choi, and J. Copeland, "An Efficient Authentication Scheme for Security and Privacy Preservation in V2I Communications," in *Proceeding of the 72nd Vehicular Technology Conference Fall (VTC-Fall)*. IEEE, Sep. 2010, pp. 1–6.

[14] H. Guo, F. Yu, Z. Zhang, W.-C. Wong, M. Ma, and Y. Wu, "HASVC: An Efficient Hybrid Authentication Scheme for Vehicular Communication," in *Proceeding of the International Conference on Communications (ICC)*. IEEE, Jun. 2011, pp. 1–5.

[15] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Flooding-resilient Broadcast Authentication for VANETs," in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking (MobiCom)*. New York, NY, USA: ACM, 2011, pp. 193–204.

[16] A.-N. Shen, S. Guo, D. Zeng, and M. Guizani, "A Lightweight Privacy-Preserving Protocol using Chameleon Hashing for Secure Vehicular Communications," in *Proceeding of IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, April 2012.

[17] H. Krawczyk and T. Rabin, "Chameleon signatures," in *Network and Distributed System Security Symposium*, 2000.

[18] G. Ateniese and B. de Medeiros, "Identity-based chameleon hash and applications," 2004.

[19] G. S. I. Blake and N. Smart, *Elliptic Curves in Cryptography*. Cambridge University Press, 1999.

[20] "The network simulator - ns-2." [Online]. Available: http://www.isi.edu/nsnam/ns/

[21] J. Härri, F. Filali, C. Bonnet, and M. Fiore, "Vanetmobisim: generating realistic mobility patterns for vanets," in *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks (VANET)*, New York, NY, USA: ACM, 2006, pp. 96–97.

[22] "2006 Second Edition TIGER/Line® Files." [Online]. Available: http://www.census.gov/geo/www/tiger/tiger2006se/tgr2006se.html

[23] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," *IEEE Communications Letters*, vol. 14, no. 1, pp. 54 –56, 2010.

[24] M. Scott, "Efficient implementation of crytographic pairings." [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf

[25] P. Muhlethaler, A. Laouiti, and Y. Toor, "Comparison of Flooding Techniques for Safety Applications in VANETs," in *Proceeding of the 7th International Conference on ITS (ITST)*. IEEE, Jun. 2007, pp. 1–6.

[26] G. Ciccarese, M. De Blasi, P. Marra, C. Palazzo, and L. Patrono, "On the Use of Control Packets for Intelligent Flooding in VANETs," in *Proceeding of Wireless Communications and Networking Conference (WCNC)*. IEEE, Apr. 2009, pp. 1–6.

[27] S. Biswas, M. Haque, and J. Misic, "Privacy and anonymity in vanets: A contemporary study," *Ad Hoc & Sensor Wireless Networks*, vol. 10, no. 2-3, pp. 177–192, 2010.

[28] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing." Springer-Verlag, 2001, pp. 213–229.

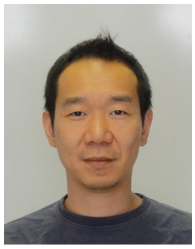
[29] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An Efficient Message Authentication Scheme for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357 –3368, Nov. 2008.

[30] S. Galbraith, K. Paterson, and N. Smart, "Pairings for cryptographers," *Discrete Applied Mathematics*, vol. 156, no. 16, pp. 3113–3121, 2008.

[31] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248 –262, Jan. 2011.

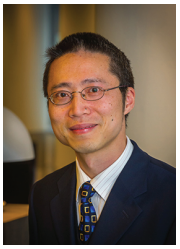
[32] D. Chaum and E. Van Heyst, "Group signatures," in *Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT)*. Berlin, Heidelberg: Springer-Verlag, 1991, pp. 257–265.

[33] S. Jiang, X. Zhu, and L. Wang, "A conditional privacy scheme based on anonymized batch authentication in vehicular ad hoc networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2013, pp. 2375–2380.



Song Guo (M'02-SM'11) received the PhD degree in computer science from the University of Ottawa, Canada in 2005. He is currently a Senior Associate Professor at School of Computer Science and Engineering, the University of Aizu, Japan. His research interests are mainly in the areas of protocol design and performance analysis for reliable, energy-efficient, and cost effective communications in wireless networks. Dr. Guo serves as associate editor of the IEEE Transactions on Parallel and Distributed Systems, Wireless Networks (Springer), Wireless Communications and Mobile Computing (Wiley), etc. He is a senior member of the IEEE and the ACM.

Deze Zeng received his Ph.D. and M.S. degrees in computer science from University of Aizu, Aizu-Wakamatsu, Japan, in 2013 and 2009, respectively. He is currently a research assistant in University of Aizu, Japan. He received his B.S. degree from School of Computer Science and Technology, Huazhong University of Science and Technology, China in 2007. He is a member of IEEE. His current research interests include cloud computing, networking protocol design and analysis, with a special emphasis on delay-tolerant networks and wireless sensor networks.



Yang Xiang received his PhD in Computer Science from Deakin University, Australia. He is currently a full professor at School of Information Technology, Deakin University. He is the Director of the Network Security and Computing Lab (NSCLab). His research interests include network and system security, distributed systems, and networking. In particular, he is currently leading his team developing active defense systems against large-scale distributed network attacks. He is the Chief Investigator of several projects in network and system security, funded by the Australian Research Council (ARC). He has published more than 130 research papers in many international journals and conferences, such as IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Information Security and Forensics, and IEEE Journal on Selected Areas in Communications. Two of his papers were selected as the featured articles in the April 2009 and the July 2013 issues of IEEE Transactions on Parallel and Distributed Systems. He has published two books, Software Similarity and Classification (Springer) and Dynamic and Advanced Data Mining for Progressing Technological Development (IGI-Global). He has served as the Program/General Chair for many international conferences such as ICA3PP 12/11, IEEE/IFIP EUC 11, IEEE TrustCom 13/11, IEEE HPCC 10/09, IEEE ICPADS 08, NSS 11/10/09/08/07. He has been the PC member for more than 60 international conferences in distributed systems, networking, and security. He serves as the Associate Editor of IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, Security and Communication Networks (Wiley), and the Editor of Journal of Network and Computer Applications. He is the Coordinator, Asia for IEEE Computer Society Technical Committee on Distributed Processing (TCDP). He is a Senior Member of the IEEE.