Efficient and Spontaneous Privacy-Preserving Protocol for Secure Vehicular Communication

Hu Xiong[†,††], Konstantin Beznosov[†], Zhiguang Qin[††], Matei Ripeanu[†]
[†]Department of Electrical and Computer Engineering,
The University of British Columbia, Vancouver, BC, Canada
[††]School of Computer Science and Engineering,
University of Electronic Science and Technology of China, Chengdu, P.R. China
Email: {xionghu,qinzg}@uestc.edu.cn, {beznosov,matei}@ece.ubc.ca

***Abstract*—This paper introduces an efficient and spontaneous privacy-preserving protocol for vehicular ad-hoc networks based on revocable ring signature. The proposed protocol has three appealing characteristics: First, it offers *conditional privacy-preservation*: while a receiver can verify that a message issuer is an authorized participant in the system only a trusted authority can reveal the true identity of a message sender. Second, it is *spontaneous*: safety messages can be authenticated locally, without support from the roadside units or contacting other vehicles. Third, it is *efficient*: it offers fast message authentication and verification, cost-effective identity tracking in case of a dispute, and has low storage requirements. We use extensive analysis to demonstrate the merits of the proposed protocol and to compare it with previously proposed solutions.**

I. Introduction

To reduce the number and the severity of crashes and to improve driving experience, car manufactures and the telecommunication industry recently have geared up to equip each vehicle with wireless devices that allow vehicles to communicate with each other as well as with the roadside infrastructure [1]. These wireless communication devices installed on vehicles, also known as onboard units (OBUs), and the roadside units (RSUs), form a self-organized Vehicular Ad Hoc Network (VANET) [3]. VANETs inherently provide a way to collect traffic and road information from vehicles, and to deliver road services including warnings and traffic information to users in the vehicles.

Extensive research efforts have been made by both industry and academia to investigate key issues in VANETs [4], [5], with security and privacy preservation as two primary concerns [6]–[11]. Without security and privacy guarantees, attacks may jeopardize the VANET's benefits: an attack, such as modification and replay of the disseminated messages, could be fatal to some users. Meanwhile, an attacker could trace the locations of the vehicles and obtain their moving patterns if user-related private information is not protected. Hence, providing privacy-preserving safety message[1] authentication has become a fundamental design requirement in securing VANETs.

The goals of privacy preservation and accountability are conflicting. On the one hand, a well-behaved OBU is willing to offer as much local information as possible to neighboring OBUs and RSUs to create a safer driving environment on condition that its privacy is protected. On the other hand, a malicious OBU may abuse the privacy protection mechanism. This may particularly happen when a driver involved in a dispute event of safety messages attempts to avoid legal responsibility. Therefore, the privacy-preserving message authentication in VANETs should be *conditional*, such that only a trusted authority can disclose the real identity of a targeted OBU in case of a traffic event dispute, even though the OBU itself is not traceable by the public.

The existing security and privacy solutions for VANETs can mainly be categorized into three classes. The first one is based on a large number of pseudo-anonymous keys (denoted as LAB in the following) [3], [8]. The second one is based on a pure group signature (denoted as GSB in the following) [7], while the last one employs the RSUs to assist with message authentication (denoted as RSUB in the following) [9], [10]. Finally, hybrid pseudonym-based approaches [11] have been proposed by combining the baseline pseudonym scheme [3] and the group signature scheme [7] together. However, these approaches can be categorized as GSB since they suffer the same drawbacks.

Though all of these solutions can meet the conditional privacy requirement, they face obstacles in real deployments. First, the LAB scheme is not efficient in terms of used storage and dispute solving. The reason is that sufficient numbers of certificates must be issued for each vehicle to maintain anonymity over a significant period of time. As a result, the certificate database to be searched by an authority in order to match a compromised certificate to its owners identity becomes a scalability bottleneck. Second, although the GSB scheme does not require each vehicle to store a large number of anonymous keys, the time for message verification grows linearly with the number of revoked vehicles. Worse, the unrevoked vehicles have to update their private keys and group public keys with the group manager when the number of revoked vehicles surpasses some predefined threshold. This problem may be fatal for VANET as they scale to cover all

[1] A *safety message* reports on the state of the sender vehicle, e.g., its location, speed, heading, etc.

vehicles in a country/continent. Finally, the RSUB protocol achieves much better efficiency than the previous ones, however, the cost of deploying RSUs is high and partial coverage is likely especially at the initial deployment stage of a VANET. For a comprehensive study of related work we refer the readers to the accompanying technical report [19].

To address these issues, this paper proposes an efficient and spontaneous conditional privacy preserving protocol for intervehicle communication based on **R**evocable **R**ing **S**ignature [18], called RRSB. Compared to previous message-authentication schemes [3], [6]–[10], our scheme has the following features: (1) *Conditional privacy*: Using the revocable ring signature to secure the intervehicle communication, preserves privacy regarding user identity and location of the vehicle, and the identities of the target vehicles can be only revealed by a trusted authority. (2) *Efficiency*: The proposed protocol can efficiently deal with a growing revocation list, it does not reply on large storage space at each vehicle or updating the group public key and private key of all unrevoked vehicles. In addition, the proposed protocol provides fast message authentication and verification and an efficient conditional privacy tracking mechanism. (3) *Spontaneity*: Safety messages can be authenticated locally, without support from the roadside units or contacting other vehicles in our protocol. (4) *Multilevel privacy*: The proposed protocol supports multiple levels of privacy, and each vehicle can independently choose his own level. The adaptivity of our protocol gives users a choice in determining their privacy requirement. We believe this protocol is an excellent candidate to secure the future VANETs.

The remainder of this paper is organized as follows. Section II presents the problem formulation, system architecture, and design objectives. Section III details the proposed security protocol, followed by the security analysis and the performance analysis in Section IV and Section V, respectively. Section VI concludes the paper.

II. Preliminaries

A. System Model

The considered system includes two types of entities: the Transportation Regulation Center (TRC), and the moving vehicles equipped with OBUs.

- OBU: All vehicles need to be registered with the TRC and preloaded with public system parameters and their own private key before they can join the VANETs. The use of secret information such as private keys generates the need for a tamper-proof device in each vehicle. The access to this device is restricted to authorized parties. OBUs are mobile and moving most of the time. When the OBUs are on the road, they regularly broadcast routine safety messages to help drivers get a better awareness of their environment and take early action to respond to an abnormal situation. Compared with the RSUs, the population of OBUs in the system could be up to millions, whereas the number of RSUs is at most tens of thousands based on the national infrastructure construction.

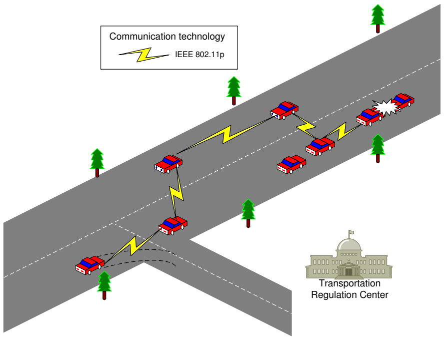

Fig. 1. System model: Road Emergency Operation under VANET

- TRC: TRC is in charge of the registration of OBUs each vehicle is equipped with. The TRC can reveal the real identity of a safety message sender whenever there is a situation where the involved vehicles' IDs need to be revealed. The TRC has sufficient computation and storage capability, and is fully trusted by all parties in the system.

Unlike other schemes, our solution does not employ RSUs. The network dynamics are characterized by quasi-permanent mobility, high speeds, and (in most cases) short connection times between neighbors. The medium used for communications between neighboring OBUs is 5.9 GHz Dedicated Short Range Communication (DSRC) IEEE 802.11p [12].

B. Objectives

Due to the space limit, we refer the readers to [3] for a full discussion of the attacker model. In the context of this work, we focus on the following objectives.

1) Efficient anonymous authentication of safety messages: The proposed scheme should provide an *efficient* and *anonymous* message authentication mechanism. First, all accepted messages should be delivered unaltered, and the origin of the messages should be authenticated to guard against impersonation attacks. Meanwhile, from the perspective of vehicle owners, it may not be acceptable to leak personal information. Therefore, providing a secure yet anonymous message authentication is critical to the applicability of VANETs.
2) Efficient tracking of the source of a disputed safety message: An important and challenging issue in these conditions is enabling TRC to retrieve a vehicle's real identity from its pseudo identity when a signature is in dispute or when the content of a message is bogus. Otherwise, an insider can launch a bogus message spoofing attack or an impersonation attack successfully. Consequently, to prevent inside attacks, it is necessary to provide traceability of safety messages.
3) Multilevel Anonymity: Privacy is a user-specific requirement and some users may be more concerned about their privacy than others. Thus, the proposed protocol should support multiple anonymity levels, and each vehicle should be allowed to independently choose its own level.

C. Bilinear Maps

Since bilinear maps [13] are the basis of our proposed scheme, we briefly introduce them here. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order q. Let P be a generator of $\mathbb{G}_1$. Suppose there exists a computable bilinear map $\hat{e}$ such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the following properties:

1) Bilinearity: For all $P_1, P_2 \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}_q$, $\hat{e}(aP_1, bP_2) = \hat{e}(P_1, P_2)^{ab}$.
2) Non-degeneracy: $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$.

Such an admissible bilinear map $\hat{e}$ can be constructed by the modified Weil or Tate pairing on elliptic curves. For example, the Tate pairing on MNT curves [14] gives the efficient implementation, and the representations of $\mathbb{G}_1$ can be expressed in 161 bits when the order q is a 160-bit prime. By this construction, the discrete logarithm problem in $\mathbb{G}_1$ can reach 80-bit security level.

D. Ring Signature

The ring signature scheme, introduced by Rivest, Shamir and Tauman [16], is characterized by two main properties: anonymity and spontaneity. Anonymity in ring signature means 1-out-of-n signer verifiability, which enables the signer to keep anonymous in these "rings" of diverse signers. Spontaneity is a property which makes the distinction between ring signatures and group signatures [13]. Group signatures allow the anonymity of a real signer in a group to be revoked by a trusted party called group manager. It also gives the group manager the absolute power of controlling the formation of the group. The ring signature, on the other hand, does not allow anyone to revoke the signer anonymity, while allowing the real signer to form a group (also known as a ring) arbitrarily without being controlled by any other party. Since Rivest *el al.*'s scheme, many ring signature schemes have been proposed.

Recently, Liu et al. [18] have introduced a new variant for the ring signature, the revocable ring signature. This scheme allows a real signer to form a ring arbitrarily while allowing a set of authorities to revoke the anonymity of the real signer. In other words, the real signer will be responsible for what has been signed as the anonymity is revocable by authorities while the real signer still has the freedom on ring formation. We use this scheme as the basis for our protocol.

III. Efficient and Spontaneous Vehicular Communications Scheme

This section describes in detail our efficient and spontaneous privacy-preserving protocol for VANETs. Each vehicle dynamically collects the messages (each message includes a set of public keys) from other vehicles it encounters during its journey. In this way, the vehicle can extract the public keys from the message and form a set of public keys for itself. We remark that that the size of this set is fixed. The vehicle will update this set of public keys after receiving the new message and the old keys in this set are discarded after the update. Through this way, this set of public keys keeps changing over time. To authenticate a message, a vehicle's OBU uses this set of public keys as its own group members to generate the revocable ring signature. This message can be anonymously authenticated by any vehicle participating in the system by verifying this signature (the only information needed for verification is the set of public keys). Finally, only by the trusted authority can reveal the identity of a signed message sender using its own private key.

The proposed scheme includes the following four phases: system initialization, OBU safety message generation and sending, OBU safety message verification, and OBU fast tracking algorithm. The notations used throughout this paper are listed in Table I.

TABLE I
NOTATIONS

Notations	Descriptions
V_i:	The ith vehicle
$\mathbb{G}_1$, $\mathbb{G}_2$:	two cyclic groups of same order q
$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$:	a bilinear map
P:	The generator of $\mathbb{G}_1$
RID_i :	The real identity of the vehicle V_i
ID_i :	The pseudo-identity of the vehicle V_i
M :	A message sent by the vehicle V_i
x_i :	The private key of the vehicle V_i
$y_i = x_i P$:	The corresponding public key of the vehicle V_i
x_{TRC}:	The private key of the TRC
$y_{TRC} = x_{TRC} P$:	The corresponding public key of the TRC
$\mathcal{H}(\cdot)$:	A hash function such as $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{Z}_q$
$a \parallel b$	String concatenation of a and b

A. System Initialization

Similar to other systems [3], [7]–[10], we assume that each vehicle is equipped with a tamper-proof device, which is secure against any compromise attempt in any circumstance. With the tamper-proof device on vehicles, an adversary cannot extract any data stored in the device including key material, data, and codes. We assume that a trusted Transportation Regulation Center (TRC) is in charge of checking the vehicle's identity, and generating and pre-distributing the private keys to the vehicle. Prior to the network deployment, the TRC sets up the system parameters for each OBU as follows:

- The TRC first randomly chooses $x_{TRC} \in_R \mathbb{Z}_q$ as its private key, and computes $y_{TRC} = x_{TRC}P$ as its public key. The TRC also chooses a secure cryptographic hash function $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{Z}_q$.
- The TRC generates a public and private key pair (x_i, y_i) for each vehicle V_i with real identity RID_i as follows: By using x_{TRC}, the TRC first computes $x_i = \mathcal{H}(x_{TRC}, RID_i) \in \mathbb{Z}_q$, and then sets $y_i = x_i P \in \mathbb{G}_1$. In the end, the TRC stores (y_i, RID_i) in its records.
- Each vehicle is preloaded with the system's public parameters $\{\mathbb{G}_1, \mathbb{G}_2, q, y_{TRC}, \mathcal{H}\}$. In addition, the tamper-proof device of each vehicle is preloaded with its private/public key pair (x_i, y_i) and corresponding anonymous certificates (these certificates are generated by taking the vehicle's pseudo-identity ID_i). Finally, the vehicle will preload the revocation list (RL) from the TRC.

B. OBU Safety Message Generation

Vehicle V_π signs the message M before sending it out. Suppose $S = \{y_1, \cdots, y_n\}$ is the set of public keys collected by vehicle V_π and it defines the ring of unrevoked public keys. Note that the public key set S, collected and stored temporarily by V_π, is dynamic. We assume that all public keys y_i, $1 \leq i \leq n$ and their corresponding private keys x_i's are generated by TRC, and π $(1 \leq \pi \leq n)$ is the index of the actual message sender. In other words, as V_π travels through the road network, the set of public keys collected by it keeps changing over time. Otherwise, a static set of public keys used by a vehicle may enable the adversary to infer its traveling trajectory. The signature generation algorithm $Sig(S, x_\pi, y_{TRC}, M)$ is carried out as follows.

1) Randomly select $r \in_R \mathbb{Z}_q$ and compute $R = rP$.
2) For y_{TRC}, compute $E_{TRC} = \hat{e}(y_\pi, y_{TRC})^r$.
3) Generate a non-interactive proof $SPK(1)$ as follows: $SPK\{\alpha : \{E_{TRC} = \hat{e}(R, y_{TRC})^\alpha\} \bigwedge \{\bigvee_{i \in [1,n]} y_i = \alpha P\}\}(M)$. The signature σ of M with respect to S and y_{TRC} is $(R, E_{TRC}, SPK(1))$.

Instantiation of SPK(1)

For clear presentation, we divide $SPK(1)$ into two components:

$$\begin{cases} SPK\{\alpha : E_{TRC} = \hat{e}(R, y_{TRC})^\alpha\}(M), & \text{(1a)} \\ SPK\{\alpha : \bigvee_{i \in [1,n]} y_i = \alpha P\}(M). & \text{(1b)} \end{cases}$$

To generate a transcript of $SPK(1a)$, given E_{TRC}, R, y_{TRC}, the actual message sender indexed by π proves the knowledge of x_π such that $E_{TRC} = \hat{e}(R, y_{TRC})^{x_\pi}$ by releasing (s, c) as the transcript such that

$$c = \mathcal{H}(y_{TRC} \parallel R \parallel E_{TRC} \parallel \hat{e}(R, y_{TRC})^s E_{TRC}^c \parallel M)$$

This can be done by randomly picking $l \in_R \mathbb{Z}_q$ and computing

$$c = \mathcal{H}(y_{TRC} \parallel R \parallel E_{TRC} \parallel \hat{e}(R, y_{TRC})^l \parallel M)$$

and then setting $s = l - cx_\pi \bmod q$.

To generate the transcript of $SPK(1b)$, given S, the actual message sender indexed by π, for some $1 \leq \pi \leq n$, proves the knowledge of x_π out of n discrete logarithms x_i, where $y_i = x_i P$, for $1 \leq i \leq n$, without revealing the value of π. This can be done by releasing $(s_1, \cdots, s_n, c_1, \cdots, c_n)$ as the transcript such that $c_0 = \sum_{i=1}^n c_i \bmod q$ and

$$c_0 = \mathcal{H}(S \parallel s_1 P + c_1 y_1 \parallel \cdots \parallel s_n P + c_n y_n \parallel M).$$

To generate this transcript, the actual message sender first picks randomly $l \in_R \mathbb{Z}_q$ and $s_i, c_i \in_R \mathbb{Z}_q$ for $1 \leq i \leq n$, $i \neq \pi$, then computes

$$\begin{aligned} c_0 \;=\; & \mathcal{H}(S \parallel s_1 P + c_1 y_1 \parallel \cdots \parallel s_{\pi-1} P + c_{\pi-1} y_{\pi-1} \parallel lP \parallel \\ & s_{\pi+1} P + c_{\pi+1} y_{\pi+1} \parallel \cdots \parallel s_n P + c_n y_n \parallel M) \end{aligned}$$

and finds c_π such that $c_0 = c_1 + \cdots + c_n \bmod q$. Finally the actual message sender sets $s_\pi = l - c_\pi x_\pi \bmod q$.

TABLE II

MESSAGE FORMAT FOR OBU

Payload	Timestamp	Signature	Public Key Sets
100 bytes	4 bytes	40n+60 bytes	20n bytes

Now we combine the constructions of $SPK(1a)$ and $SPK(1b)$ together. The transcript of $SPK(1)$ is generated as follows. First, the actual message sender randomly picks $l_1, l_2 \in_R \mathbb{Z}_q$ and $s_i, c_i \in_R \mathbb{Z}_q$ for $1 \leq i \leq n$, $i \neq \pi$, then computes

$$\begin{aligned} c \;=\; & \mathcal{H}(S \parallel y_{TRC} \parallel R \parallel E_{TRC} \parallel \hat{e}(R, y_{TRC})^{l_1} \parallel \\ & s_1 P + c_1 y_1 \parallel \cdots \parallel s_{\pi-1} P + c_{\pi-1} y_{\pi-1} \parallel l_2 P \parallel \\ & s_{\pi+1} P + c_{\pi+1} y_{\pi+1} \parallel \cdots \parallel s_n P + c_n y_n \parallel M). \end{aligned}$$

After that, the actual message sender sets $s = l_1 - cx_\pi \bmod q$, finds c_π such that $c = c_1 + \cdots + c_n \bmod q$, and sets $s_\pi = l_2 - c_\pi x_\pi \bmod q$. The transcript of $SPK(1)$ is therefore $(s, s_1, \cdots, s_n, c_1, \cdots, c_n)$.

The format of messages in our protocol is defined in Table II. According to [2], the payload of a safety message is 100 bytes. The first two fields are signed by the vehicle, by which the "signature" field can be derived. A timestamp is used to prevent the message replay attack. The last field is the public key sets, which records the public key pairs employed by the OBU.

C. Message Verification

Once a message is received, the receiving vehicle first checks if the $RL \bigcap S \overset{?}{=} \emptyset$. If so, the receiver performs signature verification by verifying of $SPK(1)$ as follows:

$$\begin{aligned} \sum_{i=1}^n c_i \;\overset{?}{=}\; & \mathcal{H}(S \parallel y_{TRC} \parallel R \parallel E_{TRC} \parallel \\ & \hat{e}(R, y_{TRC})^s E_{TRC}^{\sum_{i=1}^n c_i} \parallel s_1 P + c_1 y_1 \parallel \\ & \cdots \parallel s_n P + c_n y_n \parallel M). \end{aligned}$$

After that, the receiving vehicle updates its own public key set by randomly choosing public keys from S.

D. OBU fast tracing

A membership tracing operation is performed when solving a dispute, where the real ID of a signature generator is desired. The TRC first checks the validity of the signature and then uses its private key x_{TRC} and determines if

$$E_{TRC} \overset{?}{=} \hat{e}(y_i, R)^{x_{TRC}}$$

for some i, $1 \leq i \leq n$.

If the equation holds at, say when $i = \pi$, then the TRC looks up the record (y_π, RID_π) to find the corresponding identity RID_π meaning that vehicle with identity RID_π is the actual message generator. The TRC then broadcasts the (y_π, RID_π) to all OBUs and each OBU adds the y_π into his local revocation list (RL).

IV. Security Properties

We analyze the security of the proposed scheme in terms of the following four aspects: message authentication, user identity privacy preservation, traceability by the TRC, and spontaneity of the signature generator.

- *Message authentication*. In the proposed scheme, the ring signature can only be generated by the valid ring members. Without knowing any of the discrete logarithms x_i of the public keys y_i in the ring S, it is infeasible to forge a valid ring signature.
- *Identity privacy preservation*. Given a valid ring signature σ of some message, it is computationally difficult to identify the actual signer by any participant in the system except the TRC. If there exists an algorithm which breaks the signer anonymity of the construction in Section III, then the Indistinguishability Based Bilinear Decisional Diffie-Hellman assumption would be contradicted [18].
- *Traceability*. Given the signature, only the TRC who knows x_{TRC}, can trace the real identity of a message sender using the OBU tracking procedure described in section III-D. Besides, the tracing process carried by the TRC does not require any interaction with the message generator.
- *Spontaneity*. Note that the actual message generator can specify the ring (a set of vehicles) required to generate the ring signature arbitrarily based on the public keys of vehicles it encountered in the past without any new interaction with any other vehicles or RSUs in the system.
- *Multilevel privacy.* Each vehicle can select the degree of privacy that fits its own requirements by choosing the number of public keys used in the message generation phase. This way, each vehicle can achieve the desired balance between privacy protection and resource usage.

V. Performance Evaluation

This section evaluates the performance of the proposed scheme in terms of storage requirements and computational overheads. An extensive analysis can be found in the technical report [19].

A. Storage Overheads

This subsection compares the OBU storage overhead of our protocol with three previously proposed protocols: LAB [3], RSUB [10] and GSB [7]. In the LAB protocol, each OBU stores not only its own N_{okey} anonymous key pairs, but also all the anonymous public keys and their certificates in the revocation list (the notations adopted in the description are listed in Table III). Let each key (with its certificate) occupy one storage unit. If there are m OBUs revoked, then the scale of revoked anonymous public keys is $m \cdot N_{okey}$. Thus, the total storage overhead in LAB protocol (denoted as S_{LAB}) is $S_{LAB} = (m+1)N_{okey}$. Assuming that $N_{okey} = 10^4$, we have $S_{LAB} = (m+1)10^4$. Both in our protocol and GSB protocol, each OBU stores one private key issued by the trusted party, and m revoked public keys in the revocation list. Let S_{GSB} and S_{RRSB} denote the total storage unit of GSB protocol and our protocol (Revocable Ring Signature Based protocol) respectively. Thus, $S_{GSB} = S_{RRSB} = m + 1$. In the RSUB protocol [10], each OBU stores one private key issued by the trusted party, and a short-time key pair together with its anonymous certificate issued by the RSU. Since the OBU does not need to store the revocation list, the storage overhead in RSUB protocol is only two units, denoted as $S_{RSUB} = 2$.

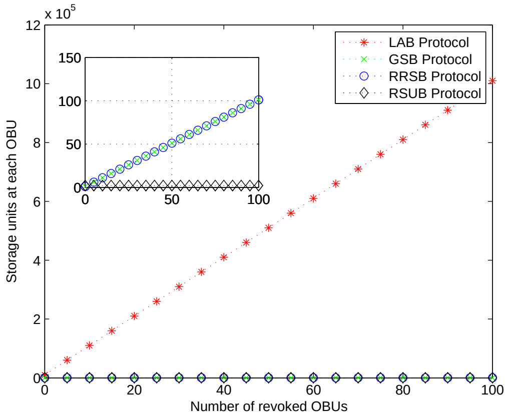

Fig. 2. Each OBU storage overhead of LAB, GSB, RSUB and RRSB in different m revoked OBUs, m varying from 1 to 100

Fig.2 shows the storage requirements of LAB, GSB, RSUB and our protocol as m increases. Observe that the OBU storage overhead in LAB protocol linearly increases with m, and is much larger than that in the other three protocols. The storage overhead of GSB protocol and our protocol is still small in spite of its linear increase with m. Though the storage overhead in RSUB protocol is the most efficient, this scheme requires the RSUs, instead of OBUs, to store the anonymous key pairs, which is not the case in the other schemes.

TABLE III
Notations and Estimated Scale

	Descriptions	Scale
N_{obu} :	The number of OBUs in the system	$O(10^7)$
N_{okey} :	The number of anonymous keys owned by one OBU	$O(10^4)$
N_{rsu} :	The number of RSUs in the system	$O(10^4)$
N_{rkey} :	The number of anonymous keys processed by one RSU	$O(10^4)$

TABLE IV
Cryptographic Operation's Execution Time

	Descriptions	Execution Time
T_{pmul}	The time for one point multiplication in $\mathbb{G}$	0.6 ms
T_{pair}	The time for one pairing operation	4.5 ms

B. Message Verification Overhead

This subsection compares the OBU computation overhead for the proposed, RSUB and GSB protocols. Since the point multiplication in $\mathbb{G}$ and pairing computations dominates each party's computation overhead, we consider only these operations in the following estimation. Table IV gives the measured processing time (in milliseconds) for an MNT curve [14] of embedding degree $k = 6$ and 160-bit q. The implementation was executed on an Intel pentium IV 3.0 GHz machine [15].

In our proposed protocol, verifying a message, requires $T_{pair} + (2n+1)T_{pmul}$, where n is the cardinality of the ring. Let T_{RRSB} be the required time cost in our protocol, then we have: $T_{RRSB} = T_{pair} + (2n+1)T_{pmul}$

In the GSB protocol, the time cost to verify a message is related to the number of revoked OBUs in the revocation list. Thus the required time is: $T_{GSB} = 6T_{pmul} + (4+m)T_{pair}$

In the RSUB protocol, to verify a message, it requires $3T_{pair} + 11T_{pmul}$. Let T_{RSUB} be the required time cost in RSUB's protocol, then we have: $T_{RSUB} = 3T_{pair} + 11T_{pmul}$

Let $T_{RG} = \frac{T_{RRSB}}{T_{GSB}}$ be the cost ratio between our proposed protocol and the GSB protocol. We observe that the time cost ratio T_{RG} decreases as m increases, which demonstrates the better efficiency of our protocol compared to the GSB protocol especially when the revocation list is large. Note that n can be determined by the user according to its own computation capacity and privacy requirements.

Let $T_{RR} = \frac{T_{RRSB}}{T_{RSUB}}$ be the cost ratio between our proposed protocol and RSUB protocol. We observe that the time cost ratio T_{RR} increases as n increases, which demonstrates our protocol is slightly more expensive than RSUB. However, our protocol does not employ the roadside infrastructures to communicate with the OBU as in RSUB, which will cause additional communication overhead.

C. Computation Complexity of OBU Tracing

We evaluate the computation complexity of OBU tracing algorithm at the trusted authority. We use the same notations as in the previous sections. The trusted authority tracking algorithm in our proposed protocol RRSB is $O(log(N_{obu}))$, the same as for the GSB protocol. The other two protocols have lower efficiency. First, the LAB protocol stores a much larger number of keys at the TRC leading to a $O(log(N_{obu} \cdot N_{okey}))$ complexity. Second, the RSUB protocol allocates at each RSU a temporary certificate for each passing vehicle in its range. In these conditions, reliably investigating road events requires aggregating all the certificates mapping produced by RSU at the TRC. Thus, the RSUB protocol will generate much higher vehicle identity tracking overheads than all the other three protocols mentioned before.

VI. Summary

We have presented an efficient, spontaneous, conditional privacy preserving protocol based on the revocable ring signature and aimed for secure vehicular communications. We demonstrate that proposed protocol does not only provide conditional privacy, a critical requirement in VANETs, but also able to improve efficiency in terms of the number of keys stored at each vehicle, identity tracking in case of a dispute, and, most importantly complexity of message authentication and verification. Meanwhile, our proposed solution can operate independently: does not require support from the roadside infrastructure which, at least in the initial deployment stages, may not cover all road segments.

References

[1] Vehicle infrastructure integration. U.S. Department of Transportation, [Online]. Available: http://www.its.dot.gov/index.htm

[2] U.S. Department of Transportation, National Highway Traffic Safety Administration, *Vehicle Safety Communications Project*, Final Report. Appendix H: WAVE/DSRC Security, April 2006.

[3] 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, Vol. 15, Nr. 1, pp. 39 - 68, 2007.

[4] T. K. Mak, K. P. Laberteaux and R. Sengupta, "A Multi-Channel VANET Providing Concurrent Safety and Commercial Services," in *Proceedings of 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, Cologne, Germany, Sep. pp. 1-9, 2005.

[5] Q. Xu, T. Mak, J. Ko and R. Sengupta, "Medium Access Control Protocol Design for Vehicle-Vehicle Safety Messages," *IEEE Transactions on Vehicular Technology*, March 2007, Vol. 56, No. 2, pp. 499-518.

[6] Y. Xi, W. Shi, L. Schwiebert. "Mobile anonymity of dynamic groups in vehicular networks", *Security and Communication Networks*, Vol. 1, No.3, pp. 219-231, 2008.

[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(6), pp. 3442-3456, 2007.

[8] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho and X. Shen, "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving", *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4987-4998, 2008.

[9] C. Zhang, X. Lin, R. Lu and P.-H. Ho. RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks. IEEE International Conference on Communications (ICC'08), Beijing, China, May 19-23, 2008.

[10] R. Lu, X. Lin, H. Zhu, P.-H. Ho and X. Shen. "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", *The 27th IEEE International Conference on Computer Communications (INFOCOM 2008)*, April 15-17, 2008.

[11] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy, "Efficient and robust pseudonymous authentication in VANET", *Vehicular Ad Hoc Networks* pp. 19-28, 2007.

[12] *Dedicated Short Range Communications* (5.9 GHz DSRC), Available: http://www.leearmstrong.com/DSRC/DSRCHomeset.htm.

[13] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," In *J. Kilian, editor, CRYPTO 2001*, volume 2139 of LNCS, pages 213-229. Springer, 2001.

[14] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals*, Vol.E84-A, No.5, pp.1234-1243, 2001.

[15] M. Scott, "Efficient Implementation of Cryptographic pairings", [on-line]. Availabe: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf

[16] R. L. Rivest, A. Shamir, Y. Tauman, "How to Leak a Secret", In *AsiaCrypt 2001*, volume 2248 of LNCS, pp. 552-565.

[17] D. Boneh, X. Boyen, H. Shacham, "Short group signatures", In: Franklin, M.K. (ed.) CRYPTO 2004. vol 3152 of LNCS, pp. 4155, Springer, Heidelberg (2004).

[18] D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo, D.S. Wong: "Revocable Ring Signature", *J. Comput. Sci. Technol.* 22(6): pp. 785-794. 2007.

[19] H. Xiong, M. Ripeanu, Z. Qin, Efficient and Spontaneous Privacy-Preserving Protocol for Secure Vehicular Communications, http://arxiv.org/abs/0909.1590, Sep 2009.