Efficient and Spontaneous Privacy-Preserving Protocol for Secure Vehicular Communications

Hu Xiong†‡, Matei Ripeanu†, Zhiguang Qin†

†School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, P.R. China
‡Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, Canada
Email: xionghu.uestc@gmail.com, matei@ece.ubc.ca, qinzg@uestc.edu.cn

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 by offering fast message authentication and verification, cost-effective identity tracking in case of a dispute, and low storage requirements. We use extensive analysis to demonstrate the merits of the proposed protocol and to contrast it with previously proposed solutions.

I. INTRODUCTION

Each year, over six million crashes occur on U.S. highways. These accidents kill more than 42,000 people, injure three million others, and cost more than $230 billion per year[1]. To reduce the number and the severity of these crashes and to improve driving experience, car manufacturers 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[2], [4]. 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)[5], [10]. 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[5], [6], [7], with security and privacy preservation as two primary concerns[10], [11], [12], [13], [14], [15], [16], [17], [18], [8], [9]. Without security and privacy guarantees, attacks may jeopardize the VANET’s benefits: a malicious attack, such as a modification and replay attack on 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 has not been protected. Hence, providing privacy-preserving safety message authentication has become a fundamental design requirement in securing VANETs.

The goals of privacy and liability 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 has been well protected. On the other hand, a malicious OBU may abuse the privacy protection mechanism. This may particularly happen when a driver who is involved in a dispute event of safety messages may attempt to avoid legal responsibility. Therefore, the privacy-preserving message authentication in VANET should be conditional, such that a trusted authority can disclose the real identity of 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 anonymous keys (denoted as LAB in the following)[11], [14], the second one is based on a pure group signature (denoted as GSB in the following)[12], [13], while the last one employs the RSU to assist vehicle in authenticating messages (denoted as RSUB in the following)[15], [16], [17]. 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. 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 revoked vehicles have to update their private key and group public key 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 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 thus only some of the roads can

1A safety message reports on the state of the sender vehicle, e.g., its location, speed, heading, etc.
2At the moment, there are in the order of some hundreds of millions of cars registered world wide
be covered especially at the initial deployment stage of the VANET. Therefore, this solution may not be feasible in case of the absence of the RSU.

To address these issues, this paper proposes an efficient and spontaneous conditional privacy preservation protocol for intervehicle communication based on revocable ring signature[34]. Compared to previous message-authentication schemes[10], [11], [12], [13], [14], [15], [16], [17], [18], [8], [9], our scheme has the following unparalleled features: (1) Conditional privacy: Using the revocable ring signature to secure the intervehicle communication, enables preserving privacy regarding user identity and location of the vehicle, and the identities of the target vehicles can be only revealed by the trusted authority; (2) Efficiency: The proposed protocol can efficiently deal with a growing revocation list instead of relying on a large storage space at each vehicle or updating the group public key and private key at all unrevoke vehicles; (3) Spontaneity: The proposed protocol does not employ RSUs to assist vehicles in authenticating messages while providing fast message authentication and verification and an efficient conditional privacy tracking mechanism. We believe this protocol is an excellent candidate for the future VANETs.

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

II. BACKGROUND AND RELATED WORK

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 the vehicle 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, such as position, current time, direction, speed, traffic conditions, traffic events, to help drivers get a better awareness of their environment and take early action to respond to an abnormal situation (Fig. 1). 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.

- TRC: TRC is in charge of the registration all 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)[21] IEEE 802.11p.

B. Related Work

Many studies have been reported on the security and privacy-preservation issues for VANETs[10], [11], [12], [13], [14], [15], [16], [17], [18], [8], [9]. Xi et al.[8], [9] introduced a random key-set-based authentication protocol to preserve the vehicle’s privacy. However, they only provide the unconditional anonymity without an effective and efficient tracking mechanism. To achieve both message authentication and conditional anonymity, Raya et al.[10], [11] introduced a security protocol in VANETs, namely LAB protocol, by requiring a large number of private keys and corresponding anonymous certificates to be installed at each vehicle. A vehicle randomly selects one of these anonymous certificates and uses its corresponding private key to sign each launched message. The other vehicles use the public key of the sender enclosed in the anonymous certificate to authenticate the source of the message. These anonymous certificates are generated by employing the pseudo-identity of the vehicles, instead of taking any real identity information of the drivers. Each certificate has a short life time to meet the drivers’ privacy requirement. Although LAB protocol can effectively meet the conditional privacy requirement, it is inefficient and may become a scalability bottleneck. Because 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 is huge.

Subsequently, Lin et al.[14] developed a time-efficient and secure vehicular communication scheme (T SVC) based on the TESLA (Timed Efficient Stream Loss-tolerant Authentication)[22]. With T SVC, a vehicle first broadcasts a
commitment of hash chain to its neighbors and then uses the elements of the hash chain to generate a message authentication code (MAC) with which other neighbors can authenticate this vehicles’ following messages. Because of the fast speed of MAC verification, the communication and computation overhead of TSVC has been reduced significantly. However, TSVC also requires a huge set of anonymous public/private key pairs as well as their corresponding public key certificates to be preloaded in each vehicle. Furthermore, TSVC is not robust when the dynamics of traffic becomes large since a vehicle should broadcast its key chain commitment much more frequently.

Lin et al.[12], [13] proposed a security protocol, i.e. GSB protocol, based on the group signature[28]. With GSB, only a private key and the group public key are stored in the vehicle, and the messages are signed according to the group signature scheme without revealing any identity information to the public. This assures that the trusted authority is equipped with the capability of exposing the identity of a sender. However, the time for safety message verification grows linearly with the number of revoked vehicles in the revocation list. Hence, each vehicle has to spend more time on safety message verification. Furthermore, when the number of revoked vehicles in the revocation list is larger than some threshold, the protocol requires every remaining vehicle to calculate a new private key and group public key based on the exhaustive list of revoked vehicles whenever a vehicle is revoked. The means for system parameters to be effectively updated to remaining vehicles, in a reliable and scalable fashion, is not explored and represents an important obstacle to the success of this scheme.

Recently, Zhang et al.[15], [16] proposed a novel RSU-aided message authentication scheme, that is RSUB, which makes RSUs responsible for verifying the authenticity of messages sent from vehicles and for notifying the results back to vehicles. In this scheme, the vehicles have lower computation and communication overhead than the previous reported schemes. Independently, Lu et al. [17] introduced an efficient conditional privacy preservation protocol in VANETs by the generation of on-the-fly short-time anonymous keys between vehicles and RSUs, which also can provide fast anonymous authentication and privacy tracking. Both of these schemes explore an important feature of VANETs by employing RSUs to assist vehicles in authenticating messages. However, RSUs may not cover all the roads, especially in the initial VANETs deployment stage, or due to the physical damage of some RSUs, or simply for economic considerations.

III. PRELIMINARIES

A. Objectives

To avoid reinventing the wheel, we refer the readers to other works[12], [11] for a full discussion of the attacker model. In the context of this work, we focus on the following security 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, including identity and location, while authenticating messages. Therefore, providing a secure yet anonymous message authentication is critical to the applicability of VANETs. Furthermore, the proposed scheme should be efficient in terms of fast verification on the safety messages and minimal anonymous keys storage at OBUs.

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, anonymous authentication only can prevent an outside attack, but cannot deal with an inside one. That is to say, an insider can launch a bogus message spoofing attack or an impersonation attack successfully if the identity of the message sender can not be traced by the authorities. So it is necessary to provide traceability for the safety message to prevent the inside attack, otherwise concerns about the security may prevent vehicle owners from joining this system.

3) Multilevel Anonymity[8]: Privacy is a user-specific requirement and some users may be more serious about their privacy than others. Thus, it is noted that the proposed protocol should support multiple anonymity levels, and each vehicle should be allowed to choose its own anonymity level. The authentication protocol should provide a tradeoff between the anonymity level and resource utilization.

B. Bilinear Maps

Since bilinear maps[23] are the basis of our proposed scheme, we briefly introduce them here.

Let \( G_1 \) and \( G_2 \) be two cyclic groups of prime order \( q \). Let \( P \) be a generator of \( G_1 \). Assume that the discrete logarithm problem in both \( G_1 \) and \( G_2 \) is hard. Suppose there exists a computable bilinear map \( \hat{e} \) such that \( \hat{e} : G_1 \times G_1 \rightarrow G_2 \) with the following properties:

1) Bilinearity: For all \( P_1, P_2 \in G_1 \), and \( a, b \in \mathbb{Z}_q \), \( \hat{e}(aP_1, bP_2) = \hat{e}(P_1, P_2)^{ab} \).

2) Non-degeneracy: \( \hat{e}(P, P) \neq 1_{G_2} \).

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[24] gives the efficient implementation, and the representations of \( G_1 \) can be expressed in 161 bits when the order \( q \) is a 160-bit prime. By this construction, the discrete logarithm problem in \( G_1 \) can reach 80-bit security level.
C. Ring Signature

The ring signature scheme, introduced by Rivest, Shamir and Tauman [26], 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 [27], [28]. 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 ring arbitrarily without being controlled by any other party. Since Rivest et al.’s scheme, many ring signature schemes have been proposed [29], [30], [31], [32], [33].

Recently, Liu et al. [34] have introduced a new variant for the ring signature, called 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 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 efficient and spontaneous conditional privacy-preservation protocol.

IV. EFFICIENT AND SPONTANEOUS VEHICULAR COMMUNICATIONS SCHEME

This section describes in detail our efficient and spontaneous privacy-preserving protocol for VANET. Each vehicle dynamically collects the public keys of other vehicles it encounters during its journey. Noted that this set of public keys keeps changing over time. When the OBU wants to send a message, it uses these public keys as its own group members to generate the revocable ring signature. Furthermore, the identity of the sender can only be recovered by the trusted authority.

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 notation used throughout this paper is listed in Table I.

A. System Initialization

Firstly, as described in section II-A, we assume 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 [11], [18]. We assume that there is a trusted Transportation Regulation Center (TRC) which is in charge of checking the vehicle’s identity, and generating and pre-distributing the private keys of the vehicles. Prior to the network deployment, the TRC sets up the system parameters for each OBU as follows:

- Let $G_1$, $G_2$ be two cyclic groups of same order $q$. Let $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a bilinear map.
- The TRC first randomly chooses $x_{TRC} \in R Z_q$ as its private key, and computes $y_{TRC} = e^{x_{TRC}}$ as its public key. The TRC also chooses a secure cryptographic hash function $H : \{0,1\}^* \rightarrow Z_q$.
- 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 $y_{TRC}$, the TRC first computes $x_i = H(x_{TRC}, RID_i) \in Z_q$, and then sets $y_i = x_i P \in G_1$. In the end, the TRC stores the $(y_i, RID_i)$ in its records.
- Each vehicle is preloaded with the public parameters $\{G_1, G_2, q, y_{TRC}, H\}$. In addition, the tamper-proof device of each vehicle is preloaded with its private/public key pairs $(x_i, y_i)$ 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 $V_\pi$ signs the message $M$ before sending it out. Suppose $S = \{y_1, \cdots, y_n\}$ is the set of public keys collected by vehicle $V_\pi$ and it defines the ring of unrevoked public keys. Note that the public key set $S$, collected and stored temporarily by $V_\pi$, 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 it $(1 \leq \pi \leq n)$ is the index of the actual message sender. In other words, $V_\pi$ travels through the road network, the set of public keys collected by it keeps changing over time. Otherwise, a unique 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 $r \in R Z_q$ and compute $R = r P$.
2) For $y_{TRC}$, compute $E_{TRC} = \hat{e}(y_{\pi}, y_{TRC})^r$.
3) Generate a non-interactive proof $SPK(1)$ as follows:
   
   $SPK\{\alpha : \{E_{TRC} = \hat{e}(R, y_{TRC})^\alpha \} \bigwedge_{i=1}^{n} y_i = \alpha P\}(M)$. The signature $\sigma$ of $M$ with respect to $S$ and $y_{TRC}$ is $(R, E_{TRC})$ and the transcript of $SPK(1)$.

| Notations | Descriptions |
|-----------|-------------|
| TRC: | Transportation Regulation Center |
| RL: | Revocation List |
| $V_i$: | The $i$th vehicle |
| $G_1, G_2$: | two cyclic groups of same order $q$ |
| $P$: | The generator of $G_1$ |
| $RID_i$: | The real identity of the vehicle $V_i$ |
| $ID_i$: | The pseudo-identity of 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 |
| $y_{TRC} = e^{x_{TRC}}$: | The corresponding public key of the TRC |
| $H(\cdot)$: | A hash function such as $H : \{0,1\}^* \rightarrow Z_q$ |
| $a || b$: | String concatenation of $a$ and $b$ |
For clear presentation, we divide $SPK(1)$ into two components:

$$SPK\{\alpha : E_{TRC} = \hat{e}(R, y_{TRC})^\alpha\}(M),$$ \hfill (1a)$$

$$SPK\{\alpha : \bigvee_{\pi\in[1,n]} y_i = \alpha P\}(M).$$ \hfill (1b)$$

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

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

This can be done by randomly picking $i \in_R Z_q$ and computing

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

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

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

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

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

$$c_0 = \mathcal{H}(S \mid s_1 P + c_1 y_1 \mid \cdots \mid s_{\pi-1} P + c_{\pi-1} y_{\pi-1} \mid l P \mid s_{\pi+1} P + c_{\pi+1} y_{\pi+1} \mid \cdots \mid s_n P + c_n y_n \mid M)$$

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

Now we combine the constructions of $SPK(1a)$ and $SPK(1b)$ together. First, the actual message sender randomly picks $l_1, l_2 \in_R Z_q$ and $s_1, c_1 \in_R Z_q$ for $1 \leq i \leq n$, $i \neq \pi$, then computes

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

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

C. Message Verification

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

$$\sum_{i=1}^{n} c_i = \mathcal{H}(S \mid y_{TRC} \mid R \mid E_{TRC} \mid \hat{e}(R, y_{TRC})^s \sum_{i=1}^{n} c_i \mid s_1 P + c_1 y_1 \mid \cdots \mid s_n P + c_n y_n \mid M).$$

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 the signature generator is desired. The TRC first checks the validity of the signature and then uses its private key $x_{TRC}$ and determines if $E_{TRC} \not\equiv \hat{e}(y_i, R)^{x_{TRC}}$ for some $i, 1 \leq i \leq n$.

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

V. SECURITY ANALYSIS

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.** Message authentication is the basic security requirement in vehicular communications. 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 $\sigma$ 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 IV, then the Indistinguishability Based Bilinear Decisional Diffie-Hellman assumption would be contradicted[34].

- **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 IV-D. Besides, the tracing process carried by the TRC does not require any interaction with the message generator. Instead, the revocable ring signature itself provides the authorship information to TRC. Therefore, once a signature is in dispute, the TRC has the ability to
trace the disputed message, in which the traceability can be well satisfied.

- **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. Compared with the schemes [15], [16], [17], our scheme does not use the RSUs to assist vehicles in authenticating messages.

- **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 a proper balance between privacy protection and resource usage. The multilevel privacy of our scheme gives users flexibility in defining their privacy requirements.

**VI. PERFORMANCE EVALUATION**

This section evaluates the performance of the proposed scheme in terms of storage requirements and computational overheads.

**A. Storage Overheads**

This subsection compares the OBU storage overhead of our protocol with three previously proposed protocols: LAB[11], RSUB[17] and GSB[12]. 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 II). 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 $N_{okey} = 10^3$, 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[17], 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 shows the storage units of LAB protocol, GSB protocol, RSUB protocol 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, nonetheless, is not the case in the other schemes.

**B. Message Verification Overhead**

This subsection compares the OBU computation overhead for the proposed, RSUB and GSB protocols. Since the point multiplication in $G$ and pairing computations dominates each party’s computation overhead, we consider only these operations in the following estimation. Table III gives the measured processing time (in milliseconds) for an MNT curve[24] of embedding degree $k = 6$ and 160-bit $q$. The implementation was executed on an Intel pentium IV 3.0 GHz machine[25].

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

$$T_{RRSB} = T_{pair} + (2n + 1)T_{pmul} = 4.5 + (2n + 1) \times 0.6(\text{ms})$$

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:

$$T_{GSB} = 6T_{pmul} + (4 + m)T_{pair} = 6 \times 0.6 + (4 + m) \times 4.5(\text{ms})$$

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:

$$T_{RSUB} = 3T_{pair} + 11T_{pmul} = 3 \times 4.5 + 11 \times 0.6 = 20.1(\text{ms})$$

Let

$$T_{RG} = \frac{T_{RRSB}}{T_{GSB}}$$
TABLE III
CRYPTOGRAPHY OPERATION’S EXECUTION TIME

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

![Fig. 3](image1.png)

Fig. 3. Time efficiency ratio $T_{RG} = T_{RRSB}/T_{GSB}$ with a number of $m$ revoked OBUs, $m$ varying from 1 to 100.

be the cost ratio between our proposed protocol and the GSB protocol. Fig.3 plots the time cost ratio $T_{RG}$ when $m$ OBUs are revoked, as $m$ ranges from 1 to 100. We observe that the time cost ratio $T_{RG}$ decreases as $m$ increases, which demonstrates the much better efficiency of our proposed protocol than 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. Fig.4 plots the time cost ratio $T_{RR}$ when $n$ public key pairs are employed, where the number of $n$ ranges from 1 to 50. We observe that the time cost ratio $T_{RR}$ increases as $n$ increases, which demonstrates our protocol is slightly more expensive than RSUB protocol. However, our protocol does not employ the roadside infrastructures to communicate with the OBU as in RSUB protocol, which will cause additional communication overhead.

C. Trusted Authority Computation Complexity on OBU Tracing

In this subsection, we evaluate the trusted authority computation complexity on OBU tracing algorithm. For fair comparison, we use the same linear and binary search algorithms in all of these protocols. We use the same notations as in the previous sections. Table IV presents the computation complexity for the four protocols. The trusted authority tracking algorithm in our proposed protocol and GSB protocol has the better efficiency than the other two protocols.

![Fig. 4](image2.png)

Fig. 4. Time efficiency ratio $T_{RR} = T_{RRSB}/T_{RSUB}$ with a number of $n$ public key pairs, $n$ varying from 1 to 50.

TABLE IV
COMPARISON OF COMPUTATION COMPLEXITY

| Protocol | Linear search | Binary search |
|----------|---------------|---------------|
| LAB      | $O(N_{obu} \cdot N_{obu})$ | $O(\log(N_{obu} \cdot N_{obu}))$ |
| GSB      | $O(N_{obu})$ | $O(\log(N_{obu}))$ |
| RSUB     | $O(N_{rsu} + N_{rkey})$ | $O(\log(N_{rsu} \cdot N_{rkey}))$ |
| RRRB     | $O(N_{obu})$ | $O(\log(N_{obu}))$ |

VII. 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 is not only provides 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 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] Saving Lives Through Advanced Vehicle Safety Technology: Intelligent Vehicle Initiative Final Report. [Online]. Available: http://www.itsdocs.fhwa.dot.gov/PRDOP/REPTS_PR/14153_files/ivi.pdf
[2] Vehicle infrastructure integration. U.S. Department of Transportation, [Online]. Available: http://www.its.dot.gov/index.htm
[3] U.S. Department of Transportation, National Highway Traffic Safety Administration, Vehicle Safety Communications Project, Final Report. Appendix H: WAVE/DSRC Security, April 2006.
[4] J. A. Misener, “Vehicle-infrastructure integration (VII) and safety”, Intelligence, Vol. 11, No. 2, pp. 1-3, 2005.
[5] R. Bishop, “A survey of intelligent vehicle applications worldwide”, in Proceedings of the IEEE Intelligent Vehicles Symposium 2000, Dearborn, MI, USA, Oct. pp. 25-30, 2000.
