A multi-purpose Group Signature for Vehicular Network Security

Mohammad Saiful Islam Mamun
Japan Advanced Institute of Science and Technology
Ishikawa, Japan.
mamun@jaist.ac.jp

Atsuko Miyaji
Japan Advanced Institute of Science and Technology
Ishikawa, Japan.
miyaji@jaist.ac.jp

Hiroaki Takada
Graduate School of Information Science
Nagoya University, Japan
hiro@ertl.jp

***Abstract*—This paper adapts a new group signature (GS) scheme to the specific needs of a vehicular ad hoc network (VANET). We modify the Groth GS in order to meet a restricted, but arguably sufficient set of privacy properties. Note that Groth GS is secure in the dynamic group signature model of Bellare, Shi, and Zhang (BSZ) without relying on random oracle Model (ROM). Although some authentication schemes using GS are proposed for VANET, none of them satisfy all the desirable security and privacy properties. Either they follow GSs that rely on ROM, or unable to satisfy potential VANET application requirements. In particular, *link management* which allows any designated entities (e.g., RSUs in VANET) to link messages, whether they are coming from the same vehicle or a certain group of vehicles, without revealing their identities. Besides that *opening soundness* property prevents malicious accusations by the opener against some honest member of the group . By using this property, we propose a new secure application framework for value-added service providers (VSPs) in VANET. Meanwhile, a real-world VANET deployment must provide a mean to *revoke* system privileges from fraudulent vehicles like the traditional Public Key infrastructure (PKI). However, in order to achieve the aforementioned security properties together in VANET, we propose a new GS model where linkability, sound opening and revocability properties are assembled in a single scheme. The novelty of our proposal stems from extending the Groth GS by relaxing strong privacy properties to a scheme with a lightly lesser privacy in order to fit an existing VANET application requirements. In addition, we partially minimize the Groth GS scheme to expedite efficiency.**

***Keywords*: VANET application, Link Manager, Revocability, Opening soundness**

I. Introduction

Unlike traditional digital signature schemes, GS allows a vehicle to create an *anonymous* (and *unlinkable*) signature that conceals the identity of the vehicle and hence preserves privacy [1][4]. Following the foundation of GS [2], a number of different security requirements have been proposed as primitives. Consequently, BSZ-model in [3], proposes the dynamic GS scheme where members may join or leave the group dynamically. BSZ-model includes three security notions anonymity, traceability and non-frameability that implies all the previously proposed notions of security. Moreover, it separates the role of Group Manager (GM) into: *issuer* and *opener* that meet the requirement of a typical VANET environment where Motor Vehicle Division (MVD) is responsible for issuing license to vehicles (may act as *issuer*) while Traffic Security Division (TSD) is accountable for fraud prevention (may act as *opener*). Furthermore, non-frameability property (by $\mathsf{Judge}(\cdot)$ algorithm) protects the member against being falsely accused of making a signature, even if both the issuer and the opener are corrupt. We utilize this property to sketch a new application framework with value-added service providers (VSPs) in VANET. Note that, a VSP is a third party service provider that could operate as an ordinary group member with additional access to the $\mathsf{Judge}(\cdot)$ algorithm in order to verify the signature as well as the owner of the resp. signature.

We exploit the GS proposed by Groth [7] for several reasons: (1) this scheme is secure in BSZ-model, (2) it offers a constant number of group elements for *group public key* and generated *signatures* (this property is a prerequisite to support scalability), (3) it satisfies strong security requirements, that is, security proof does not rely on weak random oracle model (security proofs in the random oracle model are not sound with respect to that in the standard model). All these features may best fit to a vehicular network model.

Furthermore, security must be considered as an aspect of reliability; and the reliability of the network may lessen due to poor security policy and/or vulnerable cryptographic constructions. Authors in [6] address a security threat (*opening soundness* in [7]) to the reliability of ownership of a signature and provide a solution regarding this. Let a vehicle be registered to a VSP for a certain service. It is mandatory for a VSP to ascertain that it is providing service to the right vehicle to which it has agreement to. But lack of *opening soundness* may allow a malicious vehicle to claim for service as if it is an honest vehicle. This potential threat can be resolved by accumulating *opening soundness* to the *signature* so that by using $\mathsf{Judge}(\cdot)$ VSP can verify the identitiy of the vehicle correctly. We propose the *opener* to issue a *token* (a proof of ownership of the signature) θ on a *ticket* (message m containing service name and its signature Σ) to the vehicle for a certain service. In order to obtain services from VSPs, a vehicle must submit a valid *ticket* (m, Σ_i) together with *token* (θ) generated on it and its *identity* i. VSPs in response verify the signature Σ_i on m and the identity i of the owner of the

signature by examining the proof sealed in the *token* θ.

Although a vehicular network demands group signature schemes that exhibit strong privacy properties, but sometimes stringent privacy policy prevents some reasonable case of application. In order to guarantee vehicle privacy, group signatures can be directly used to anonymously authenticate vehicular communication. We observe that standard GSs like Groth's GS, is unsuitable for diverse privacy requirement needed for VANET. Therefore, we refer to relax strong privacy properties of Groth GS by introducing *Link manager* (LM) where a designated entity (e.g., RSU) could link the signers anonymously without revealing their identifiers. For instance, let an RSU intend to keep the record of the average number of emergency vehicles pass through a certain junction during business hours without revealing the identity of the vehicles. That is, RSUs need to track the vehicle while preserving the privacy intact. Therefore, we propose a LM to be installed in each RSU that offers linkability while preserving anonymity. When a message together with its signature has been received by the LM, it can link the message with any of the previously received messages from the same vehicle. This feature significantly introduces a privacy hierarchy in VANET from the low level *vehicles* to the upper level *opener*. More clearly, vehicles are fully anonymous in the network, RSUs can only link among vehicles but cannot circumvent anonymity, a VSP is offered to break privacy of the subscribed vehicles only, and an opener can crack full anonymity.

Note that all the aforementioned GS properties are not completely novel. Firstly, *linkability* feature is discussed in several traceable GS schemes such as [16] [17] [21] and very recently [18]. But all of them either do not support opening algorithm and hence do not allow anonymity revocation, or the security proof belongs to ROM. Secondly, *revocability* properties for a GS was first explored in [10] and later followed by [9] [22] [23]. All the revocable GS schemes have been proposed so far were either reluctant to backward unlinkability, constant signature size/ verification cost/ public key size, or rely on ROM. Recently, two scalable revocation approaches: [14] [15] have been proposed from standard security model. Since the revocation techniques are inspired by broadcast encryption tree, the cardinality of the group becomes fixed and more harshly their signature size is 6 times larger than that of our scheme which could cause performance bottleneck in a large scale VANET application. Thirdly, we followed the *opening soundness* property described in [6] which protect the signature from getting hijacked by other member vehicles.

Main contributions: We introduce a GS scheme, based on pairing-based construction of Groth with additional properties: (1) *linkability* (Link Manager in RSUs), (2) *opening soundness* (token provided by the opener) (3) *revocability* (run by Issuer and group members periodically)

We accumulate the aforementioned properties in a single scheme. In addition, for accelerating efficiency we use a simplified version of Groth GS that is CPA-secure, and later suggest applying batch verification technique for standard GS [13] for signature verification.

II. Preliminary

A. Network model

We refer to the hierarchical network model described in [1]. In this model, vehicles are remained at the bottom of the hierarchy (see Fig. 1). Vehicular groups could be formed: by region (ex. east region), social spots/services (ex. shopping mall, hospital area), category (ex. public service, emergency, personal vehicles) etc. Each vehicle in the network must be equipped with an On Board Unit (OBU) consisting of Event Data Recorder (EDR) that records all the received messages, Tamper Proof Device (TPD) that implements cryptographic tools and ensures authenticated access control. Each GM consists of an *issuer* for the purpose of registration and an *opener* (TSD) to explore the identification of vehicles. Subsequently, all the RSUs would act as LMs.

B. Extended GS Properties with prior works

1) Link Manager: Let an RSU intend to collect traffic data (e.g., frequency of emergency vehicles passing through a specific road, which type of vehicles tend to violate traffic rules such as driving over the speed limit etc.) from the road for future traffic analysis without revealing identities of the vehicles. We propose to set Link manager (LM) up into the designated RSU and create vehicular groups according to *category* (such as emergency vehicles).

Besides that, we render traceability with the help of on-demand delegated linkability as follows:

- Firstly, if any suspicious vehicle discovers a *doubtful* message arriving from a group member, it would forward the message with corresponding signature to the LM (preset in the RSUs) instead of *opener* (TSD) for revocation.
- Secondly, RSU is delegated the linking capability by the *opener* that introduces a fine-grained control on the anonymity of vehicles. By using the linking key, RSU can check if two or more doubtful messages have been arrived from the same vehicle.
- Finally, if RSU determines a specific vehicle as *malicious member*, the message together with its signature would be forwarded to the *opener* to reveal the vehicle identity. Usually an *opener* responds only to the privileged verifiers (e.g. RSUs in VANET).

Note that, Traffic Security Division (TSD) should have *policies* on how RSUs would confirm fraudulent vehicles. An example of this would be, if a certain vehicle produces several deceitful messages within a short period of time, or if a vehicle keeps sending multiple messages indicating same events on the road e.g., Sybil attack.

It is worth pointing out that *full anonymity* can not be achieved here since RSUs can link certain vehicles or a group of vehicles, and hence, *absolute privacy* can not be guaranteed. We termed this as *relaxed privacy*.

Providing linking capability to a group signature is not novel. For example, direct anonymous attestation scheme (in [16]), ring signature scheme (in [17]) hold linkability algorithm. Unfortunately, these group signature schemes do not include any traceability algorithm. However, a recently proposed

GS scheme (in [18]) has both linkabilty and traceability, but the security of the scheme is considered in the random oracle model. Moreover it cannot be guaranteed whether the scheme has *opening soundness* or not.

Note that LM can provide long-term linkability (until the group public key and linking key are refreshed). Sometimes we require short-term linkability for efficient verification with privacy. Short-lived pseudonym is one of the solutions to provide short-term linkability while protecting privacy in VANET. Here we discuss a solution to achieve short-term linkability with pseudonym mechanism. Consider several Group Managers (GMs) under a fully Trusted Party (TP) where Setup phase of each GS would be performed by TP. Each group member under a GM should use pseudonym signed by the TP instead of original identifier of a vehicle (ID_{V_i}) during Registration with *Issuer* (User i Registration at Section III). Each time TP signs a new pseudonym generated by ID_{V_i}, it ensures that the member is not already revoked.

More clearly, during Setup phase, TP chooses a signature scheme with key pair $(\mathsf{Sign}_T, \mathsf{Ver}_T)$ and public Key scheme (PK) with key pair $(\mathsf{sk}_T, \mathsf{pk}_T)$. Similarly, GM chooses PK key pair $(\mathsf{sk}_G, \mathsf{pk}_G)$. In Registration phase, first each member V_i chooses PK key pair $(\mathsf{sk}_{V_i}, \mathsf{pk}_{V_i})$ for secure communication with TP and seeks a certified pseudonym for its real identifier ID_{V_i}. In response, TP provides the pseudonym Π_i padded with expiration date (Timestamp) and its signature (encrypted by pk_{V_i}) to the member vehicle. After first successful registration to the TP, a member vehicle may update its pseudonym Π_i any time *online*. However, Issuer in Registration phase of GS uses Π_i (instead of x_i in the current scheme). Vehicles entering a new GM_i area should provide a valid pseudonym (not expired) to receive the group secret key (gsk_i) for future communication within a GM_i's area.

In this scenario, Revocation would be accomplished by the cooperation of global TP and GMs. For instance, during revocation Traffic Security Division (with Open algorithm) of GM_i can extract the member pseudonym that would be forwarded to the TP in order to extract the original ID of a vehicle (ID_{V_i}). TP then updates its global revocation list accordingly and ensures that any malicious member in the revocation list cannot update its pseudonym in the next registration phase. Later TP broadcasts updated revoked member list to all the active GMs so that they can check the temporary revoked members until the lifetime of the pseudonym expire. Hence, using pseudonym facilitates flexible linkability with expiration date (while LM provides long-term linkablity inside a group) independently of the GMs.

Furthermore, sometimes short-term linkability can be achieved by fixing some parameter during Authentication phase (with Gsign algorithm). For instance, if ρ is unchanged in our scheme in the consecutive n signatures, it will generate same $(a, \varkappa)$ (part of Σ) for n signatures. Hence, short-term linkability is accomplished.

2) Opening soundness: Groth's group signatures are susceptible to be hijacked by a malicious member by forging the *proof of ownership* generated by the *opener* [6]. We present a secure application framework by utilizing this property. For instance, let a vehicle have an agreement with a third party service provider. It would generate a message (citing the VSP's name and requested service information) with its signature (we termed it as a *ticket*) and submit them to the Traffic Security Division (conveying *opener* algorithm) for attestation. Opener would issue a proof of ownership (we termed it as a *token*) of the signature in order to bind a credential to its legitimate owner (see Fig. 1). Subsequently, later when the vehicle requests for a service to the VSP, it would attach a *ticket* and its corresponding *token* issued by the *opener*. VSPs (conveying *judge* algorithm) could justify the message with the credential of the vehicle.

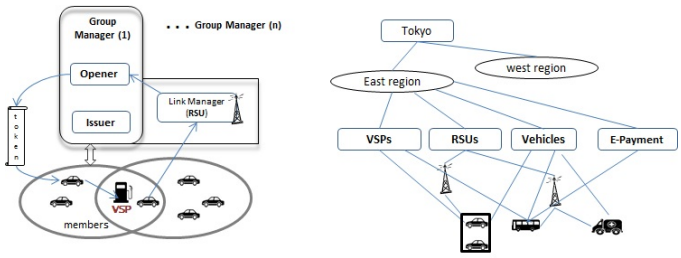

Fig. 1. An example demonstrating: vehicles' group formation (right) and communication among the GS members (left) in a traditional VANET Network.

3) Revocation: Like standard PKIs, GS does not have any efficient revocation system in practice. Many existing solutions do not scale well due to either high overhead or tight operational requirements, such that, computational complexity belongs to $O(n)$ or $O(r)$, where n and r are group size and number of revoked members respectively. Revocation solution was first introduced in [10], where the signature size was linear to the number of revoked members. Authors in [11] proposed a forward secure revocation system with constant signature size. But, one of the features of this scheme was to use fixed time periods to revoke a member, which is in fact, impossible to implement in VANET environment. Schemes in [22] [23] have $O(1)$- cost for signing and verification time but $O(n)$-size (linear) group public keys.

Recently, two revocations approaches have been proposed, mainly based on the Naor-Naor-Lotspiech (NNL) Broadcast Encryption framework that yields a scalable revocable group signatures to obtain private keys of constant size in the standard model [14] [15]. Unfortunately, signature size of both the schemes are too large for practical deployment. They are approximately 3 and 6 times larger, respectively, than that of our scheme[1]. Moreover, since NNL is a tree-based technique, unlike ordinary dynamic GS schemes the maximal cardinality of the group would be fixed. Therefore, even though the revocation schemes are truly scalable, they cannot be used for VANET application where larger signature size causes increased communication overhead and hence degrades overall performance and the number of group member vehicles should be flexible, not fixed.

We exploit the idea of [9] in our GS, where they offer a CRL-like revocation with constant length signature as well as constant computation for revocation, that means, the complexity is $O(1)$ with respect to n and r.

[1]Group signature size of [14] and [15] are comprised of 144 and 92 group elements respectively while our signature size consists of 28 group elements.

III. The Proposal

Groth GS applies *certified signature* method based on the **DLIN** and the $q-$**U** assumption (see [7] for details) using Non-interactive Witness-indistinguishable (NIWI) proofs[5]. Note that we present a relaxed (CPA-secure) notion of Groth GS e.g., allow no adversarial access to the *open* algorithm and add/modify some generic algorithm e.g., adding: SignLink(), Revoke() modifying: Keygen(), Registration(), Open() algorithms.

System Setup: Consider a probabilistic polynomial time algorithm $\mathcal{G}$ that generates $gk := (p, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e, g) \leftarrow \mathcal{G}(1^k)$ such that: p is a k-bit prime, $(\mathbb{G}, \mathbb{G}_{\mathbb{T}})$ are cyclic group of order p. Let g generate $\mathbb{G}$ and e be a non-degenerate and efficiently computable bilinear map s.t., $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$ so that $e(g, g)$ generates $\mathbb{G}_{\mathbb{T}}$, and $e(g^a, g^b) = e(g, g)^{ab}$ for any $a, b \leftarrow \mathbb{Z}_p$.

Key Generation $\mathsf{GKg}(1^k)$: Group Manager (Traffic Escrow Authority) generates secret keys: ik for Issuer (Registration managers), ok for Opener (Traffic Security Division), lk for Linker (Designated RSUs) and public system parameters gpk. Let $(u, h, z, K, L) \leftarrow \mathbb{G}$, $(l, r, s) \leftarrow \mathbb{Z}_p$, $f = u^l$, $T := e(f, z)$, $xk := (\phi, \eta) \leftarrow gk, F := g^{\phi}, H := g^{\eta}$, , $R := g^r, S = g^s$, Hash $\leftarrow \mathcal{H}(1^k)$; $\mathsf{Parse}(crs) := (F, H, therest)$. $pk := (F, H, K, L)$, $lk := l$, $ik := z$, $ok := xk$, and $gpk := (gk, \text{Hash}, u, f, h, T, crs)$

Registration (User i : gpk, Issuer: gpk, ik): Group members with their identity i (e.g., vehicles, RSUs) need to complete registration with Issuer. Let total number of non-revoked vehicles be n in an instance. A vehicle i and Issuer run a 5-move key generation protocol (described in [8]) in order to generate a key pair $\{(v_i, x_i), v_i\}$, where $v_i \leftarrow g^{x_i}$ Issuer then signs v_i to produce certificate
$\mathsf{certSign}_i := (a_i, b_i) \leftarrow (f^{-r_i}, (v_i h)^{r_i} z)$, where $r_i \leftarrow \mathbb{Z}_p$.
Vehicle i accepts the certificate $\mathsf{certSign}_i$ if $e(a_i, hv_i)$ $e(f, b_i) = T$. Finally, the Issuer maintains a database to store $reg[i] \leftarrow v_i$ for the open() and the judge() algorithm, and $rev[i] \leftarrow r_i$ for the revocation() algorithm and the vehicle i stores group signing key $gsk[i] \leftarrow (x_i, \mathsf{certSign}_i)$

Authentication $\mathsf{GSign}(gpk, gsk[i], m)$: In order to sign a message m a registered vehicle i first generates a certified signature σ using her private key x_i. Then it produces a NIWI proof[2] π that consist of a commitment to σ. The detailed instantiation is as follows. Let a vehicle i select $\rho \leftarrow \mathbb{Z}_n$ and compute $a := a_i f^{-\rho}$, $b := b_i (hv_i)^{\rho}$, $\varkappa = u^{-\rho}$ and $\sigma := g^{1/x_i + \mathcal{H}(m)}$. $\pi \leftarrow \mathrm{P}_{\text{NIWI}}$ $(crs, (gpk, a, \mathcal{H}(m)), (b, v_i, \sigma))$
The resulting signature on a message m is: $\Sigma := (a, \varkappa, \pi, \sigma)$.

Message verification $\mathsf{GVerify}(gpk, m, \Sigma)$: To verify a signature Σ on message m, receiving vehicle or RSU checks NIWI proof π:
IF $\mathrm{V}_{\text{NIWI}} \leftarrow (crs, (gpk, a, \mathcal{H}(m)), \pi) = \textit{true}$;
return 1
ELSE **return** 0

Traffic Security Division $\mathsf{Open}(gpk, ok, m, \Sigma)$: By accessing the registration table *reg*[][3] generated by the Issuer, by using opening key ok it can revoke the signer's identity i of a valid signature Σ on message m. This algorithm can be used for two purposes: Firstly, it helps to exhibit the signer of a doubtable message/signature sender and later revoke the member vehicle from the group. Secondly, it promotes accountability of certain applications by providing proof of ownership of a certain signature. Consider a member vehicle i that requires a credential regarding a service which is mentioned in the message m. The vehicle could first generate a signature Σ on m and then request the Opener() to provide a proof of ownership or token on m. After that, it could submit m to the VSP along with Σ and the token to justify. The detailed are as follows:
First, it verifies the signature by using $\mathsf{GVerify}$ (gpk, m, Σ). If successful, then it extracts v of the corresponding vehicle i and searches the registration table to find $v \stackrel{?}{=} v[i] \leftarrow reg[i]$.
$(b, v, \sigma) \leftarrow \mathsf{Extract}_{ok}(crs, (gpk, a, \mathcal{H}(m)), \pi)$.
In order to generate proof of ownership, it randomly selects $(c, d) \leftarrow \mathbb{Z}_p$ and computes: $(y_1, y_2, y_3) := (F^c, H^d, v_i g^{c+d})$ and a Non Interactive Zero Knowledge (NIZK) proof $\theta \leftarrow (\theta_1, \theta_2)$ of corresponding vehicle i where $\theta_1 := y_1^{1/\phi}$, $\theta_2 := y_2^{1/\eta}$ and $(\phi, \eta) \leftarrow ok$. Finally, it issues (i, y, σ, θ) which is termed as a proof of ownership of a signer i on a certain message m, or a *token*.

Validating Ownership $\mathsf{Judge}(gpk, i, v_i, m, \Sigma, \theta)$: This algorithm verifies whether the opening is correct or not. It returns 1 if the opening is correct. VSPs in VANET could use this algorithm to verify the beneficiary of a certain service.
IF $\Big($**GVerify**$(gpk, m, \Sigma) = 1 \bigwedge (i \neq 0) \bigwedge e(\sigma, v_i g^{\mathcal{H}(m)}) = e(g, g) \bigwedge e(F, \theta_1) = e(y_1, g) \bigwedge e(H, \theta_2) = e(y_2, g) \bigwedge \sigma\theta_1\theta_2 = y_3\Big)$
return 1
ELSE **return** 0

Managing Linkability $\mathsf{SignLink}((\Sigma_1, m_1), (\Sigma_2, m_2), lk)$: By using lk, the LM (e.g., designated RSUs in VANET) tries to find a link among existing list of signatures with a new signature, or between two signatures whether they are generated from the same signer i. It returns 1 if sucessful Let $a_1, \varkappa_1 \leftarrow \Sigma_1$ and $a_2, \varkappa_2 \leftarrow \Sigma_2$.
IF $\mathsf{GVerify}$ $(gpk, m_1, \Sigma_1) \bigwedge$ $\mathsf{GVerify}$ (gpk, m_2, Σ_2)
IF $e(a_1, h)$ $e(\varkappa_1, h^{lk})^{-1} = e(a_2, h)$ $e(\varkappa_2, h^{lk})^{-1}$ Or, $e(a_1/a_2, h) = e(\varkappa_1/\varkappa_2, h^{lk})$
return 1
ELSE **return** 0

Intuition: $\rho_i \neq \rho_j$ and $gsk[i] \neq gsk[j]$ for any (i, j)
$e(a_1/a_2, h) = e(\varkappa_1/\varkappa_2, h^{lk})$
$\Rightarrow e(a_i f^{-\rho_1}/a_i f^{-\rho_2}, h) = e(u^{-\rho_1}/u^{-\rho_2}, h^l)$
$\Rightarrow e(u, h)^{l(\rho_2 - \rho_1)} = e(u, h)^{l(\rho_2 - \rho_1)}$

[2]To demonstrate that ciphertext contains a valid certified signature

[3]The opener has read access to the registration table *reg*[]

Since $a_i \leftarrow \mathsf{certSign}(a_i, b_i)$ is randomized by ρ to generate a in $\mathsf{GSign}()$, there would be no security compromise.

Revocation $\mathsf{Revoke}(gpk, RList)$: Revocation would be accomplished in two steps: Firstly, GM issues a new group public key gpk including all new parameters, termed as $\mathcal{R}$, and publish it for all the non-revoked members. Usually, the Issuer publishes a signed and time-stamped $\mathcal{R}$ in a publicly accessible bulletin board or server. Unlike ordinary GS schemes, in our scheme vehicles do not need to contact the *issuer* privately (following interactive *join/issue* protocol) to update their certificates. Secondly, after getting the public parameters $\mathcal{R}$ for revocation, all the non-revoked member vehicles can update their certificates (a_i, b_i) with the newer one consequently. However, it is quite likely that no revoked members can update their certificates from the revocation information available in public. Moreover, all other non-revoked member vehicles need $O(1)$ operation to update, irrespective of the size of the revocation list or the group members.

This algorithm allows Issuer and all non-revoked member vehicles to update their keys according to the revoked users list $RList$ provided by the GM. Let $t := \{\prod_{i=1}^{n} r_i, s.t.\ r_i \leftarrow rev[i]\}$ be known to all the last known non-revoked n group member vehicles. Note that, t considers of all the current non-revoked members including the *new* member vehicles that join between two consecutive revocation events.

Let m member vehicles be adjudged as *illegal* vehicles between two successive revocation events, and $r_{ki} \leftarrow rev[i]$ be selected for the revoked members (m). Then, ***RList***:= $k_1, k_2 \cdots k_m$ where $m < n$; and $r_k = \prod_{i=1}^{m} r_{ki}$.

Issuer: update $rev[i]$ according to the new list of non-revoked member vehicles (n)

$\tau \leftarrow \mathbb{Z}_n; \delta := \tau^l;\ u' := u \cdot \tau;\quad f' := f \cdot \delta;\quad h' = h \cdot \delta$

$T' := e(f', z)$; and $\gamma := \delta^{\frac{t}{r_k}} \bmod n$

new $gpk := (gk, \text{Hash}, u', f', h', T', crs)$

publish $\mathcal{R} \leftarrow (t, gpk, \gamma, r_k)$ for the non-revoked members.

Member vehicle $(i \neq k_i)$: update non-revoked member's certificate $certSign_i(a_i, b_i)$:

$gsk[i] := (x_i, a_i{}', b_i{}') \leftarrow (x_i, a_i, b_i)$

set $s_i = \frac{r_i \cdot r_k}{t}$

set $a_i' = a_i \cdot \gamma^{-s_i}$ and $b_i' = b_i \cdot \gamma^{s_i}$

IV. Security Requirement

Some of the notations and security definitions we use from [7] [6] and also omit the description of security proof due to space constraint. Interested readers are referred to [7] [6] for further discussion.

Lemma 1. *Modified Groth GS satisfies the revocability under the DL-assumption and provides backward unlinkability.*

Proof: Issuer publishes $\mathcal{R} \leftarrow (t, gpk, \gamma, r_k)$ that includes group public key gpk and other necessary parameters in public. Note that, all the updated gpk parameters (u, f, h, T) are randomized by δ, and $\gamma := \delta^{(t/r_k)}$ is published as part of $\mathcal{R}$. γ is calculated only from the non-revoked members r_i (from $rev[i]$ pre-stored to Issuer). In order to sign a message, a non-revoked member need to create a valid $certSign$ by following

$$(a_i', b_i') \leftarrow (a_i * \delta^{-r_i}, b_i * \delta_i^r) \text{ s.t., } \gamma^{s_i} = \delta^{(t/r_k)*(r_i*r_k)/t}$$

However, it is impossible for a revoked member to produce new $certSign$. Because it is hard to explore δ from γ under DL-assumption. Therefore, it is hard for a PPT adversary $\mathcal{A}$ to produce a colluding non-revoked member.

Let the adversary $\mathcal{A}$ be able to link signatures generated before and after a revocation phase. Thus, in order to break backward unlinkability, $\mathcal{A}$ needs to distinguish two signatures Σ_a (generated after revocation), Σ_b (generated before revocation). It appears that Groth GS scheme provides anonymity under DLIN assumption[4]. Moreover, during each signature generation, the parameters $(a, b, \varkappa)$ are randomized by ρ, and σ is independent of the updated parameters during revocation, since it is generated from the secret x_i. Furthermore, linkability from π is also infeasible, since it is a proof from NIWI that assures indistinguishability from the secrets/witnesses it possess, based on a variant of DDH assumption. □

Lemma 2. *Modified Groth GS is linkable under DL assumption.*

Proof: We use CPA-anonymous version of the Groth GS. That is, signature is untraceable under DLIN assumption. Similarly, we assume that any PPT adversary $\mathcal{A}$ does not have access to *open*$(\cdot)$ oracle and thus does not have access to open key ok. Unlike anonymity-game, in the linkability-game $\mathcal{A}$ has access to the *linking* key lk in order to find a link among signatures from the same signer, or a group of signers while not being aware of the real signers of the signatures. However, the adversary $\mathcal{A}$ can compute a linking index: $e(a_i f^{-\rho_i}, h)$ associated with each signer i where (a_i, ρ_i) pair is associated with a signer i. Let LM create a database that is indexed by $e(a_i f^{-\rho_i}, h)$. We assume this index is singular and uniformly distributed from adversarial point of view. Clearly, this index is unique and independent of the signer's signing key $gsk[i] \leftarrow x_i$.Therefore, it is hard for a PPT adversary $\mathcal{A}$ to guess the identity i of the signer from a given signature Σ.

V. Efficiency

We minimize and exploit a simpler variant of Groth GS [7]. Therefore, we provide construction for relaxed security notions (CPA anonymity) that removes the non-essential features of the main GS. Meanwhile, we extend the existing Groth GS to satisfy some essential security notions with minor performance overhead. However, ordinary CCA-anonymous Groth GS consist of 50 group elements in $\mathbb{G}$ while the lighter version, where CPA-anonymity is sufficient and the adversary is not allowed to access *opening* oracle[5], the size of signature can be reduced to 28 group elements. Still it supports dynamic member enrollment, constant number of group elements in *keys* and *group signatures*, opening soundness, feasible revocation,

[4] A natural extension of DDH assumption

[5] In VANET, Traffic Security Division (Opener) is commonly assumed to be tamper-proof

TABLE I. VANET SECURITY PROPERTIES

	Ours	J. Hwang[18]	MSI Mamun[4]	L. Zhang[19]	W. Lingbo[20]
Security Proof	Standard	ROM	ROM	ROM	ROM
Anonymity	CPA	CPA	CCA	CPA	CPA
Linkability	Yes	Yes	No	No	No
Revocability	Yes	Yes	No	Yes	Yes
Non-frameability	Yes	Yes	Yes	Yes	No
Opening Soundness	Yes	No	No	No	No
Batch verification	Yes	No	Yes	No	Yes

linkability to achieve relaxed privacy through LM. In [4], the authors show how efficiency degrades in relation to pairing computation in VANET environment and propose some solutions to speed up the signature verification process. In [13], the authors address this challenge for Groth signature and propose a batch verification system to reduce almost 90% of the pairing calculation. However, introducing batch verification for single signature has reduced expensive pairing equation per signature from 68 to 11. While the batched version requires only $4n+7$ pairings for n signatures. In addition, introducing off-line signature scheduling algorithm to find an optimum value of the batch size n, and paralleling partial pairing calculation using *thread*, as described in [4], can further optimize the final operation time for signature verification.

However, if we allow LM to be used in each vehicle for short-term linkability, it significantly improves signature verification. As the message with signature arrives to the vehicle, it will first search the local database whether the sending vehicle is already known to it (by using LM key it can easily link the incoming signature with any previous record from the same vehicle). If the sending vehicle is enlisted already in the receiving vehicle's local database (e.g., second (or higher) message from the same sending vehicle), expensive verification part (e.g., 11 pairing calculation) can be omitted. For instance, if a receiving vehicle requires 11 pairing calculation for the first signature it has received from a vehicle i, it presumably need no pairing calculation from the second or any subsequent signatures coming from the vehicle i until no suspicious/deceitful message is claimed by the receiving vehicle. Nevertheless, over time the local database of the receiving vehicle can become enlarged that would cause performance bottleneck in database searching.

Finally, in Table 1. we compare our scheme with some other recent GS schemes proposed for VANET in terms of security properties, security proof method, Linkability, Non-frameability, Revocability, Opening Soundness and Performance etc.

VI. CONCLUSION

In this paper, we focus on hierarchical privacy-preserving among all entities of VANET by using Groth GS. We have presented a reliable and standard CPA-secure GS solution to a vehicular network application considering revocability, linkability and opening soundness. We consider the lighter version of Groth GS to enhance efficiency while preserving optimal security with several essential properties. Further, we suggest LM that provides restricted privacy appropriate for a real time VANET environment. Moreover, this can protect against DoS and Sybil attacks as well. In addition, using batch verification can significantly improve the performance of signature verification that makes the solution applicable for real life vehicular communication.

REFERENCES

[1] J. Guo, J.P. Baugh and S. Wang. A group signature based secure and privacy-preserving vehicular communication framework. In Mobile Networking for Vehicular Environments, pp. 103-108, 2007.

[2] D. Chaum and E. V. Heyst. Group signatures. In EUROCRYPT, volume 547 of Lecture Notes in Computer Science, pages 257-265, 1991.

[3] M. Bellare, H. Shi, C. Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 136-153. Springer, Heidelberg 2005.

[4] M. S. I. Mamun, A. Miyaji. An Optimized Signature Verification System for Vehicle Ad hoc NETwork, The 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM2012), IEEE, to appear.

[5] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In EUROCRYPT, volume 4965 of Lecture Notes in Computer Science, pages 415-432, 2008.

[6] Y. Sakai, J. C.N. Schuldt, K. Emura, H. Hanaoka, K. Ohta. On the security of Dynamic Group Signaturs: Preventing Signature Hijacking, LNCS 7293, pp. 715-732, PKC 2012.

[7] J. Groth. Fully Anonymous Group Signatures Without Random Oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164180. Springer, Heidelberg (2007)

[8] J. Groth. Fully anonymous group signatures without random oracles, Feb 15 (2012) (manuscript), http://www.cs.ucl.ac.uk/staff/J.Groth/CertiSignFull.pdf

[9] G. Ateniese, G. Song, and G. Tsudik. Quasi-efficient revocation of group signatures, In Financial Crypto 2002, Lecture Notes in Computer Science (LNCS), 2002.

[10] E. Bresson and J. Stern. Efficient Revocation in Group Signatures, In Proceedings of Public Key Cryptography (PKC'2001), Springer-Verlag, 2001.

[11] D. Song. Practical Forward-Secure Group Signature Schemes, In Proceedings of ACM Symposium on Computer and Communication Security. November 2001.

[12] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In CRYPTO, LNCS(3152), pages 41-55,2004.

[13] O. Blazy, G. Fuchsbauer, M. Izabachene, A. Jambert, H. Sibert, and D. Vergnaud. Batch Groth-Sahai. In Proc. ACNS 2010, volume 6123 of LNCS, pages 218-235. Springer-Verlag,2010.

[14] B. Libert, T. Peters, M. Yung. Group Signatures with Almost-for-free Revocation. CRYPTO2012, LNCS7417, pp. 571-589, 2012.

[15] B. Libert, T. Peters, M. Yung. Scalable Group Signature with Revocation. Eurocrypt2012, LNCS7237, pp 609-627, 2012.

[16] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In CCS 04, pages 132145, New York, NY, USA, 2004. ACM Press.

[17] J. Liu, W.Susilo, D. Wong. Ring signature with designated linkability. IWSEC2006, LNCS4266, pp.104-119, 2006.

[18] J. Hwang, S. Lee, B. Chung, H. Cho, D. Nyang. Short Group Signatures with Controllable Linkability. In IEEE LightSec2011, Pages: 44-52, 2011.

[19] L. Zhang, Q. Wu, B. Qin, J. Ferrer. Practical Privacy for Value-Added Applications in Vehicular Ad Hoc Networks. In IDCS2012, LNCS(7646), pp 43-56, 2012.

[20] W. Lingbo.On a Group Signature Scheme Supporting Batch Verification for Vehicular Networks. In IEEE Multimedia Information network and Security (MINES2011), pp 436-440, 2011.

[21] Chow, S. S., Susilo, W., Yuen, T. H. Escrowed linkability of ring signatures and its applications. In Progress in Cryptology-VIETCRYPT 2006 (pp. 175-192). Springer Berlin Heidelberg,2006.

[22] Libert, B., Vergnaud, D. Group signatures with verifier-local revocation and backward unlinkability in the standard model. In Cryptology and Network Security (pp. 498-517). Springer Berlin Heidelberg, 2009.

[23] Nakanishi, T., Fujii, H., Yuta, H., Funabiki, N. Revocable group signature schemes with constant costs for signing and verifying. IEICE transactions on fundamentals of electronics, communications and computer sciences, 93(1), 50-62, 2010.