Secure VANET Applications with a refined Group Signature

Mohammad Saiful Islam Mamun and Atsuko Miyaji
Japan Advanced Institute of Science and Technology (JAIST)
Ishikawa, Japan.
{mamun, miyaji}@jaist.ac.jp

***Abstract*—This paper proposes an application-friendly group signature (GS) model for wireless ad hoc network like Wireless Sensor Networks (WSN) or Vehicle ad hoc Network (VANET). Our new GS properties can be used to carry out potential solution to some real life problems. We modify Boneh, Boyen and Shacham (BBS) short GS to meet a restricted, but arguably sufficient set of privacy properties. In particular, we aggregate linking, direct opening, message-dependent opening (MDO), revoking, batch-verification in a *single* short GS scheme. Our link manager can link messages whether they are coming from the same messages or not without colluding to the *opener*. It helps relaxing strong privacy properties of GS to a lightly lesser one that fit certain application requirement. We introduce a new application to the ad hoc network security, that is, value-added service provider (VSP) with the help of MDO properties and redesign the traditional GS-friendly VANET architecture. Our revocation algorithm adapts both rekeying and verifier-local revocation (VLR) approaches to revoke illegitimate signers in a constant time. Finally, we present an optional batch verification system to expedite signature verification. Note that all these properties have already been shown in the literature scatteredly. The novelty of our proposal stems from accumulating all these properties in a single GS scheme that can best fit to the application demand.**

***Keywords*: Group signature, VANET.**

I. Introduction

Although complete untraceability (strong privacy) among the members is an important properties for applications like WSN where nodes are bounded to places or human body in order to measure data and position, or, VANET where vehicles with On Board Unit (OBU) are considered as preliminary nodes, sometimes stringent privacy policy prevents some reasonable case of application. For example, pseudonym mechanisms (e.g., [4], [17]) and GS scheme (e.g., [10], [20], [30]) are two popular approaches to guarantee privacy in VANET, but sometimes application demands diverse privacy requirement. Members might benefit from established trust relations among them in order to communicate private data in an unobservable manner [18], [19].

For better understanding, from now on we would consider our proposed solution to VANETs only. However, this solution can be applied to any ad hoc network systems where different labels of privacy, jurisdiction access, and revocability are necessary on dense communication. VANET offers two types of wireless communication, namely, V2V− communication among the vehicles, V2I− communication between vehicles and a VANET infrastructure like Road Side Unit (RSU). In this paper, we address some real life application scenarios as follows:

Scenario 1. Let a car C be registered to some Value Added Service Provider (VSP) for some special events or services (fuel filling station, garage service, auto mechanic center etc.). Generally service stations need to ensure the right client and services it had agreement to. For instance, C has subscribed to 'gasoline from filling station F' through VSP. VSP issues a *token* regarding C's subscription. When C appears physically to the service station F, it would request for the service providing the *token* it received from the VSP. Note that, a service center can expose C's identity if and only if the *token* admits the service as C is claiming for and is generated from the VSP.

Scenario 2. In *Scenario* 1, we have seen that service provider can revoke signer's anonymity depending on *token*. But in case of culprit members, such as a vehicle involved in an accident, sometimes it becomes essential for the Traffic Security Division (TSD) to forcefully revoke the signer's identity.

Scenario 3. Let an accident occur and vehicles in the vicinity of the accident start broadcasting warning messages through V2V communication. Car C that moves towards the accident area, would receive more warning messages even from the same sender including periodical broadcast messages from other vehicles. C must conceive the validity of these messages in order to decide the next route. Note that, VANET allows maximum message processing time to be 300 *ms* [20]. Using batch verification is one of the solutions to verify a batch of signatures quickly. However, batch verification is not always efficient if the number of messages to batch is not decided intelligently [10], or if the number of bogus messages in a single batch is more than 15% [16].

Scenario 4. In addition to *Scenario 3*, a signature verifier may need additional processing time when it considers local revocation check. Group signature approach with VLR (e.g., [26]) incurs expensive verification phase specially for a long-sized *revocation list*. Moreover, revocation list grows linearly with time when new revoked members are added into the list unless member keys with public parameters are reinitialized (called re-keying). Nonetheless, re-keying process is not feasible, and hence, is often pre-scheduled to get rid of the burden of communication overhead.

Scenario 5. Let a licit (may be hijacked) vehicle keep sending doubtful messages for a number of times. In general case, the messages together with signatures would be forwarded to the TSD (tracer in GS) to revoke. But it is not always wise to request TSD for every single suspicious message. It would convey serious burden to the TSD.

Main challenges in the security proposals of VANET are to connect security, privacy, efficiency and management capability. *Scenario 1-5* are some real life problems that can be solved using GS approach. Prior works in this field try to solve some of these problems scattaredly in different schemes. In this paper, we tried to solve all the aforementioned problems in a *single* scheme efficiently. To the best of our knowledge, this is a complete GS scheme from short BBS GS where almost all the GS properties (available in the literatures) are accumulated.

II. Related Work and Our Contribution

A. Related Work

Security and privacy in VANETs are discussed in the literature mainly from pseudonyms [4], [19] and group signature approaches. Unlike traditional digital signature schemes, GS allows its members to create *anonymous* (and *unlinkable*) signatures that conceal the identity of the members and hence preserves privacy [1]. Following the foundation of GS [2], a number of different security requirements have been proposed as primitives. Consequently, BBS-model in [23], proposes the shortest GS scheme mainly with three security notions-anonymity, traceability and exculpability.

Linkability feature is discussed in several GS schemes such as short GS based scheme in [28], direct anonymous attestation scheme in [25], ring signature schemes in [27], [31]. All of them do not support either traceability or revocability. In [35], authors propose a special type of GS with short-term linkability for VANET where the signer will keep remain three group signature elements unchanged (without randomizing) for a short term. Although it gears up verification process, but signatures generated this way are linkable by all the group members. Whereas, in general, linkable GS has *linking key* to link signatures and members who have linking key can only link the signatures.

Traceability is a fundamental properties of BBS GS [23]. In [15], authors introduce a new direction to traceability. In order to subside the power of the *opener*, they bring in a new authority called *admitter* which generates *tokens* corresponding to messages without which tracing manager (*opener*) cannot proceed. Once the *token* is generated, no interaction between the *opener* and the *admitter* is required for further operation. Although message-dependent traceability is more application-friendly, sometimes authorities like TSD in VANET requires to revoke a member's anonymity *directly* without depending on any other authority (e.g., emerging national security threats).

Revocability properties for a GS was first explored in [22] and later followed by [21], [33], [34]. All the revocable GS schemes that have been proposed so far are reluctant to backward unlinkability, verification cost (VLR) etc. GS scheme in [7] combines hybrid revocation mechanism with [23] that works with the list of revoked members, namely revocation list (RL), and a threshold value. If the size of RL is less than the threshold value, the scheme follows VLR scheme for revocation. Otherwise the scheme uses *re-keying* process to update the public/private group keys of all non-revoked members. In [13], authors introduce a special VLR supported GS scheme with time-bound keys. Although they minimize the revocation check to a greater extent, but the verifier still needs to perform revocation check against all the members in RL. Note that VLR scheme with RL is not practical for a large scale VANET where a verifier needs to check whether a signer belong to the RL each time it receives a signature.

In [12], authors propose a GS with batch verification with drawbacks like impersonation attack, tractability etc. [8]. A short GS based on [23] and an Identity Based Group Signature (IBGS) based on [11] with fast batch verification are proposed in [6] and [10] for a large scale VANET. Authors show how the performance of batch verification degrades in dense/sparse communication.

B. Main contributions

We introduce a short GS scheme based on [23] with additional properties for a large scale VANET: (1) selective linkability, (2) direct traceability, (3) message-dependent traceability, (4) hybrid revocability with constant computation. Our proposed solution is more application-friendly than the related works. Clearly, we focus on solving some real-life problems described in *Scenario 1-5* efficiently.

- We propose two new authorities, namely Admitter and Linker before revoking a signer's anonymity. Linker can partially break anonymity by linking the signatures from the same signer (without exploring member identification) while Admitter assists Opener to break full anonymity (by exposing member identification). It introduces a fine-grained control on the anonymity of the members.
- We suggest two different algorithms for traceability, namely Direct tracing and Attested tracing. Direct tracing algorithm can trace any signer directly with its own key. On the other hand, Attested tracing algorithm rely on the *token* issued by Admitter to trace a signer [15].
- We introduce a hybrid revocation algorithm with limited VLR and rekeying process. To avoid the inefficient checking of RL during signature verification, our proposal uses 0/1 *encoding*-enabled signing and verfication and the expired-date bound signing key [13]. This encoding system enables *set intersection* predicate in [9]. With this property, if there is a common element between two sets of encoded expired dates (signer's key and signature), verifier will pass the signature.
- To solve *Scenario 1*, in V2I communication, our proposal uses the modified scheme of [15]. For value added service, let a vehicle C request VSP (Message attestation

authority) to generate a *token* T_c regarding the service (e.g., fueling) to subscribe. When C will go into the subscribed service station e.g., fuel filling station (Attested tracing authority), first it verify the signature on service, later, it will check whether the token T_c was generated by VSP on the same service. Note that it can only expose C's identity if and only if T_c admits the service C is claiming for.

- To solve *Scenario 2*, in I2I communication, RSU will request TSD (Direct Tracing authority) with culprit member's generated message and signature who can forcibly revoke signer's identity.
- To solve *Scenario 3*, in V2V communication, verifier should first check whether batch verification is feasible for the current situation following algorithm in [10]. If yes, it uses efficient batch verification process to verify a bunch of signatures together. In addition, it can adapt categorized verification (in [35]) by providing linking key (Managing linkability algorithm) to the vehicle where the signatures from the *known* vehicles are batched together in order to resist bogus messages in the batch. Note that the verifier recognizes a vehicle to be known if the incoming signature is linkable to the former signature it received.
- To solve *Scenario 4*, we propose the revocation system to comply with both VLR and rekeying process. To optimize the cost of VLR checking we propose a revocability-enabled credentials with natural expiration date that is generally used for authentication in mobile roaming [14]. It helps the verifier to ascertain that the message is not generated by an expired signer key at a *fixed* cost. We use the modified VLR scheme from [13]. Note that our limited version of VLR is more efficient, but do not consider the members that are forcedly revoked prematurely. Nonetheless, our rekeying system from [5] will take care of that. This hybrid approach will lead to a substantial reduction (constant) on revocation check (for each message) specially in a situation where prematurely revoked credentials are very few in number.
- To solve *Scenario 5*, we propose a novel solution with short-term linkability where vehicle will forward messages with signatures to some designated entity like RSU. Let an RSU have the linking key and a counter q. It increases the counter value by 1 after it receives any suspicious message from the identical vehicle (by linking signatures). According to some preset value of the counter, RSU would finally request the TSD to revoke the member from the group.

To the best of our knowledge, there is no GS scheme proposed in the literature that satisfy all the aforementioned properties together. We accumulate the cited properties in a single scheme and this challenging effort helps to induce relaxation from a strong privacy to a scheme with a lesser but adaptive privacy hierarchy, and hence make the GS scheme applicable to certain application environment by being simplistic, yet efficient way.

III. Preliminary

A. Network model and Scheme Description

We refer to a symbolic hierarchical network model for VANET described in Fig.1. It consists of a Trusted System (TS), a Group Manager (GM), Traffic Security Division (TSD), Value-added Service Provider (VSP), Service Station (SS), and Members (Vehicle, RSU). Vehicular groups could be formed by region, social spots/services, vehicle category etc. Each vehicle in the network is equipped with an On Board Unit (OBU) consisting of an Event Data Recorder (EDR) that records all the received messages and a Tamper Proof Device (TPD) that implements cryptographic tools. Three types of communication exist in the network: Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) and Infrastructure to Infrastructure (I2I).

- TS creates and manages the groups in the network. It generates the public parameters for cryptographic operation.
- GM manages the registration of the members such as vehicles, RSUs by providing group secret keys with expiration date. It is securely connected to other pertaining authorities like VSP, TSD, SS. It periodically announces the new group public key for revocation (rekeying). We assume the GM to be honest and secure. However, it cannot reveal any member's identification.
- Admitter works for the Attested Trace authority. It generates token for the vehicles according to their subscription.
- Attested trace authorities are service stations (SS) approved by GM. It provides services to the subscribed vehicles upon receiving the token generated by Admitter (VSP).
- Direct Trace authority is securely connected with RSUs. It can trace and open the member's identity upon request (by the designated RSUs).
- Members includes RSUs and vehicles with embedded OBUs. They collect certificates from GM during registration. Vehicles can communicate with other vehicles through V2V communication. Moreover, they can communicates with RSU through V2I communication to report any malicious message (vehicles are not allowed to communicate directly to TSD).

B. 0/1-ENCoding and VLR

In [9], authors present an encoding scheme, namely $0/1$-encoding, that helps converting the *greater than* predicate to the *set intersection* predicate. This property allows the GM to embed the *key expiration* date into the signer's certificate and the signer to sign a message with a *signature expiration* date. Since the signer should not expose its key expiration date d (for privacy purpose), it sets an expiration date t (such that $d > t$) for each signature. Later verifier can check if the current date $\bar{t}$ is no later than the signature expiration date t. It ensures ($d > t \geq \bar{t}$) that the signature is generated by a non-expired signer. Clearly, verifier will pass the signature

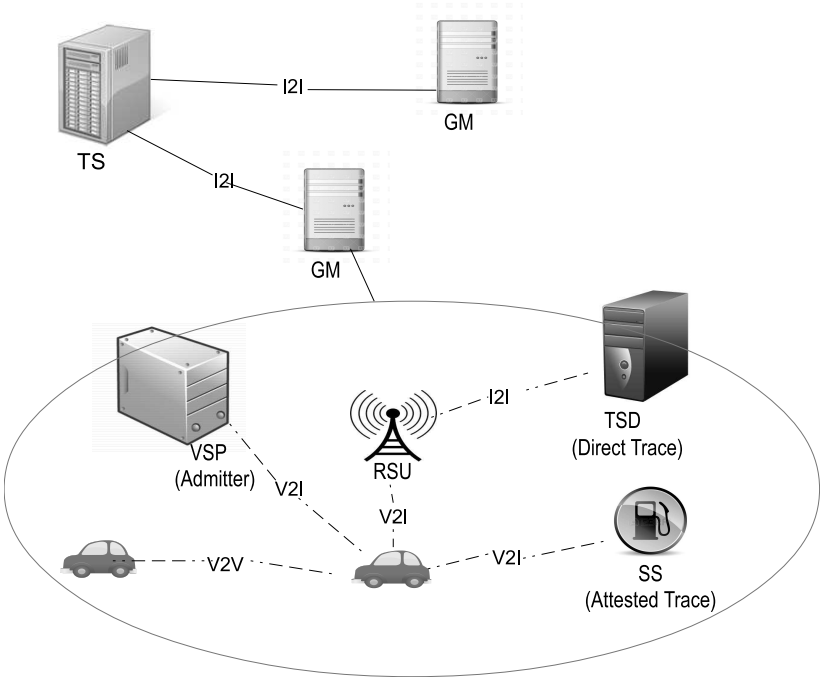

Fig. 1. VANET Security Model.

if there exists a common element between the signer's (key) expiration date and signature expiration date.

It converts a date format (in binary) to a value in $\mathbb{Z}_p$ in the following way.

- Let $t \leftarrow t_{[l]} \dots t_{[1]}$ be an l-bit date encoded in binary string.
- 0-Enc: $T_t^0 = \{t_{[l]} \dots t_{[i+1]}\mathbf{1} \| t_{[i]} = 0, 1 \le i \le l\}$,
  1-Enc: $T_t^1 = \{t_{[l]} \dots t_{[i]} \parallel t_{[i]} = 1, 1 \le i \le l\}$.
- If $x > y$, there is a common element in T_x^1 and T_y^0.

- To ensure that the sets start with 1, redefine the sets as the decimal number set as follows
  $\overline{T_t^0} = \{1 \cdot 10^{l-i+1} + t_{[l]} \cdot 10^{l-i} + \dots + t_{[i+1]} \cdot 10^1 + 1 \| t_{[i]} = 0, 1 \le i \le l\}$,
  $\overline{T_t^1} = \{1 \cdot 10^{l-i+1} + t_{[l]} \cdot 10^{l-i} + \dots + t_{[i+1]} \cdot 10^1 + t_{[i]} \| t_{[i]} = 1, 1 \le i \le l\}$,

- Padding with dummy elements so that the number of elements in the sets are same.
  For 0-Enc:

$$t_{[i]} = \begin{cases} z & \text{if } z \in \overline{T_t^0} \text{ and } \lfloor \log_{10} z \rfloor - 1 = i \\ 2 \cdot 10^i & \text{otherwise,} \end{cases}$$

  For 1-Enc:

$$t_{[i]} = \begin{cases} z & \text{if } z \in \overline{T_t^1} \text{ and } \lfloor \log_{10} z \rfloor - 1 = i \\ 3 \cdot 10^i & \text{otherwise.} \end{cases}$$

- Assume two dates x = "10100010111" ('1303' for March,2013) and y = "1010001010" ('1301' for January,2013) in a format 'YYMM'. Now

  $T_x^1 = \{1, 101, 1010001, 101000101, 1010001011, 10100010111\}$,
  $T_y^0 = \{11, 1011, 10101, 101001, 10100011, 1010001011\}$ and

  $\overline{T_x^1} = \{11, 1101, 11010001, 1101000101, 11010001011, 110100010111\}$,
  $\overline{T_y^0} = \{111, 11011, 110101, 1101001, 110100011, 11010001011\}$

- After padding
  0-Enc$(y) \rightarrow \{20, 111, 2000, 11011, 110101, 1101001, 20000000, 110100011, 2000000000, \mathbf{11010001011}, 200000000000\}$,
  1-Enc$(x) \rightarrow \{11, 300, 1101, 30000, 300000, 3000000, 11010001, 300000000, 1101000101, \mathbf{11010001011}, 110100010111\}$.

- Since $x > y$, 1-Enc(x) and 0-Enc(y) have a common element **11010001011**. For detailed proof, please find the theorem in [9].

C. The Computational Assumptions

Let $\mathcal{G}$ be a probabilistic polynomial-time algorithm that takes a security parameter 1^λ as input and generates a parameter $(p, \mathbb{G}, \mathbb{G}_T, e, g)$ of *bilinear groups*, where p is a λ-bit prime. $\mathbb{G}$ and $\mathbb{G}_T$ are groups of order p, g is a generator of $\mathbb{G}$, and e is a bilinear map: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

The DL assumption. Let $g \leftarrow \mathbb{G}$, $a \leftarrow \mathbb{Z}_p$. The Discrete Logarithm (DL) problem in $\mathbb{G}$ is stated as follows. Given (g, g^a), output (a). The advantage of a probabilistic polynomial-time (PPT) algorithm $\mathcal{A}$ against DL problem is defined as $\mathrm{Adv}_{\mathcal{A}}^{\mathsf{DL}}(\lambda) = \Pr[\mathcal{A}(g, g^a) = a]$.
We say that the DL assumption holds if $\mathrm{Adv}_{\mathcal{A}}^{\mathsf{DL}}(\lambda)$ is negligible for any algorithm $\mathcal{A}$.

The DDH assumption. Let $g \leftarrow \mathbb{G}, (a,b,c) \leftarrow \mathbb{Z}_p$. The decisional Diffie-Hellman problem (DDH) problem in $\mathbb{G}$ is stated as follows. Given (g, g^a, g^b, g^c), output 1 if $c = ab$, otherwise 0 if $c = r$. The advantage of an algorithm $\mathcal{A}$ against the DDH problem is defined as $\mathrm{Adv}^{\mathsf{DDH}}_{\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(g, g^a, g^b, g^c) = 1 \mid c = ab] - \Pr[\mathcal{A}(g, g^a, g^b, g^c) = 1 \mid c = r]|$.
We say that the decision linear assumption holds if $\mathrm{Adv}^{\mathsf{DDH}}_{\mathcal{A}}(\lambda)$ is negligible for any PPT algorithm $\mathcal{A}$.

The q-SDH assumption. Let $(p, e, g, \mathbb{G}, \mathbb{G}_T) \leftarrow \mathcal{G}(1^\lambda)$, $\gamma \leftarrow \mathbb{Z}_p$ and $A_i \leftarrow g^{\gamma^i}$ for $0 \le i \le q$. The q-strong Diffie-Hellman (SDH) problem in $\mathbb{G}$ is stated as follows. Given $(g, (A_i)_{0 \le i \le q})$, output $(c, g^{1/(\gamma+c)})$ where $c \in \mathbb{Z}_p^*$. The advantage of a PPT algorithm $\mathcal{A}$ against the q-SDH problem is defined as $\mathrm{Adv}^{q-\mathsf{SDH}}_{\mathcal{A}}(\lambda) = \Pr[\mathcal{A}(g, (A_i)_{0 \le i \le q}) = (c, g^{1/(\gamma+c)})]$.
We say that the q-SDH assumption holds if $\mathrm{Adv}^{q-\mathsf{SDH}}_{\mathcal{A}}(\lambda)$ is negligible for any algorithm $\mathcal{A}$.

The DLIN assumption. Let $(u, v, h) \leftarrow \mathbb{G}, (\alpha, \beta, r) \leftarrow \mathbb{Z}_p$ and $g_1 \leftarrow u^\alpha, g_2 \leftarrow v^\beta$. The decision linear (DLIN) problem in $\mathbb{G}$ is stated as follows. Given $(u, v, h, u^\alpha, v^\beta, z)$, output 1 if $z = h^{\alpha+\beta}$, otherwise 0 if $z = h^r$. The advantage of an algorithm $\mathcal{A}$ against the DLIN problem is defined as $\mathrm{Adv}^{\mathsf{DLIN}}_{\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(u, v, h, u^\alpha, v^\beta, z) = 1 \mid z = h^{\alpha+\beta}] - \Pr[\mathcal{A}(u, v, h, u^\alpha, v^\beta, z) = 1 \mid z = h^r]|$.
We say that the decision linear assumption holds if $\mathrm{Adv}^{\mathsf{DLIN}}_{\mathcal{A}}(\lambda)$ is negligible for any PPT algorithm $\mathcal{A}$.

The DBDH assumption. Let $(p, \mathbb{G}, \mathbb{G}_T, e, g) \leftarrow \mathcal{G}(1^\lambda)$ and $a, b, c, r \leftarrow \mathbb{Z}_p$. The decision bilinear Diffie-Hellman (DBDH) problem in $(\mathbb{G}, \mathbb{G}_T)$ is stated as follows. Given (g, g^a, g^b, g^c, z), output 1 if $z = e(g,g)^{abc}$, otherwise 0 if $z = e(g,g)^r$. The Advantage of an algorithm $\mathcal{A}$ against the DBDH-problem is defined as $\mathrm{Adv}^{\mathsf{DBDH}}_{\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(g, g^a, g^b, g^c, z) = 1 \mid z = e(g,g)^{abc}] - \Pr[\mathcal{A}(g, g^a, g^b, g^c, z) = 1 \mid z = e(g,g)^r]|$.
We say that the DBDH assumption holds if $\mathrm{Adv}^{\mathsf{DBDH}}_{\mathcal{A}}(\lambda)$ is negligible for any PPT algorithm $\mathcal{A}$.

IV. Our Proposal

Our scheme employs the GS scheme in [15] which expands the BBS GS scheme in [23] by replacing the linear encryption with multiple encryption of ordinary Public Key Encryption (PKE) and Identity based encryption (IBE). Additionally, we extend the GS with several potential functionality for VANET, such as, revocation following works in ([13], [5]), batch verification with ([16], [35], [10]) and direct traceability from [35], linkability with [28].

Let g is a generator of $\mathbb{G}$. The possession of SDH tuple is (A, x) where $A \in \mathbb{G}, x \in \mathbb{Z}_p, w = g^\gamma$ such that $A^{\gamma+x}$. This can be verified by $e(A, wg^x) = e(g,g)$. The short GS in ([23], [35]) is based on the proof of knowledge SPK:$\{(A,x) : A^{\gamma+x} = g\}(M)$. on message M. Since our secret keys are associated with an additional expiration date d, we modify the underlying signature. The possession of a tuple (A, x) such that $A^{\gamma d+x} = g$ can be verified by $e(A, w^d g^x) = e(g,g)$. Hence, SPK:$\{(A,x) : A^{\gamma d+x} = g\}(M)$.

System Setup: Consider a probabilistic polynomial time algorithm $\mathcal{G}(1^\lambda)$ with a security parameter 1^λ that generates a parameter of bilinear group $(p, \mathbb{G}, \mathbb{G}_T, e, g)$. The proposed scheme uses two hash functions $H_1 : \{0,1\}^* \to \mathbb{G}$ and $H_2 : \{0,1\}^* \to \mathbb{Z}_p$ that are modeled as random oracles in the security analysis.

Issuing Credentials $\mathsf{GKgen}(1^\lambda, 1^l, 1^n)$: On input security parameter 1^λ, the maximum length of the date format l and the maximum number of vehicles n, this algorithm selects random integers $\xi_1, \xi_2, \xi_3, \zeta, \gamma, \ell \leftarrow \mathbb{Z}_p$ and random elements $u, v, h \leftarrow \mathbb{G}\backslash\{1\}$. Then it sets $g_1 \leftarrow u^{\xi_1} h^{\xi_3}$, $g_2 \leftarrow v^{\xi_2} h^{\xi_3}$, $y \leftarrow g^\zeta$, $w \leftarrow g^\gamma$, and $f \leftarrow u^\ell$. The algorithm computes $\{d_{ij}\}_{j \in [1,l]} \leftarrow 1\text{-}\mathsf{ENC}(d_i)$, where d_i is the expiration date of a signer i. The algorithm then selects $x_{ij} \leftarrow \mathbb{Z}_p$ and sets $A_{ij} \leftarrow g^{1/(\gamma d_{ij} + x_{ij})}$ such that $\gamma d_{ij} + x_{ij} \neq 0$ for each vehicle i ($i \in [1,n]$). Finally, the algorithm outputs:

- Group public key $gpk \leftarrow (p, \mathbb{G}, \mathbb{G}_\mathbb{T}, f, e, g, u, v, h, g_1, g_2, y, w, H_1, H_2)$
- Signing key $gsk_i \leftarrow (A_{ij}, x_{ij}, d_i)_{i \in [1,n],\ j \in [1,l]}$
- Linking key $lk \leftarrow h^\ell$
- Registration table
  $reg_1[i]_{1 \le i \le n} \leftarrow \{A_{ij}, e(A_{ij}, g)\}_{i \in [1,n],\ j \in [1,l]}$
  $reg_2[i]_{1 \le i \le n} \leftarrow \{x_{ij}, e(g,g)^{x_{ij}}\}_{i \in [1,n],\ j \in [1,l]}$
- Admitter key $ak \leftarrow \zeta$
- Direct tracing key $dok \leftarrow (\ell, reg_2[i]_{1 \le i \le n})$
- Attested tracing key $aok \leftarrow (\xi_1, \xi_2, \xi_3,\ reg_1[i]_{1 \le i \le n})$

Signature Generation $\mathsf{GSign}(gpk, t, i, gsk_i, M)$: On input the group public key gpk, user i, the signing key $gsk_i \leftarrow (A_{ij}, x_{ij}, d_i)_{i \in [1,n],\ j \in [1,l]}$, the signature expiration date t, and a message M, this algorithm generates a group signature σ as follows.

- If $t \ge d_i$, output $\perp$.
- Compute $\{d_{ij}\}_{j \in [1,l]} \leftarrow 1\text{-}\mathsf{ENC}(d_i)$ and $\{t_j\}_{j \in [1,l]} \leftarrow 0\text{-}\mathsf{ENC}(t)$. Find an index $k \in [1,l]$ such that $d_{ik} = t_k$.
- Choose random $\alpha, \beta, \rho, \eta \leftarrow \mathbb{Z}_p$ and compute

$$(T_1, T_2, T_3, T_4) \leftarrow (u^\alpha, v^\beta, h^{\alpha+\beta}, g_1^\alpha g_2^\beta A_{ik} g^\eta)$$
$$(T_5, T_6, T_7) \leftarrow (g^\rho, e(y, H_1(M))^\rho e(g,g)^{-\eta}, g^{1/x_{ik}} f^\alpha)$$

- Choose blinding values randomly $r_\alpha, r_\beta, r_\rho, r_\eta, r_x, r_{\alpha x}, r_{\beta x}, r_{\rho x}, r_{\eta x} \leftarrow \mathbb{Z}_p$ and compute

$$R_1 \leftarrow u^{r_\alpha},$$
$$R_2 \leftarrow v^{r_\beta},$$
$$R_3 \leftarrow h^{r_\alpha + r_\beta},$$
$$R_4 \leftarrow e(T_4, g)^{r_x} e(g_1, w)^{-r_\alpha d_{ik}} e(g_1, g)^{-r_{\alpha x}} e(g_2, w)^{-r_\beta d_{ik}} \cdot e(g_2, g)^{-r_{\beta x}} e(g, w)^{-r_\eta d_{ik}} e(g,g)^{-r_{\eta x}},$$
$$R_5 \leftarrow g^{r_\rho},$$

$R_6 \leftarrow e(y, H_1(M))^{r_\rho} e(g,g)^{-r_\eta}$,
$R_7 \leftarrow T_1^{r_x} u^{-r_{\alpha x}}$,
$R_8 \leftarrow T_2^{r_x} v^{-r_{\beta x}}$,
$R_9 \leftarrow T_5^{r_x} g^{-r_{\rho x}}$,
$R_{10} \leftarrow T_6^{r_x} e(y, H_1(M))^{-r_{\rho x}} e(g,g)^{r_{\eta x}}$,
$R_{11} \leftarrow e(T_7, g)^{r_x} e(f,g)^{-r_{\alpha x}}$

- Compute $c \leftarrow H_2(t, M, T_1, \ldots, T_7, R_1, \ldots, R_{11})$, and then compute

$s_\alpha \leftarrow r_\alpha + c\alpha$,
$s_\beta \leftarrow r_\beta + c\beta$,
$s_\rho \leftarrow r_\rho + c\rho$,
$s_\eta \leftarrow r_\eta + c\eta$,
$s_x \leftarrow r_x + cx_{ik}$,
$s_{\alpha x} \leftarrow r_{\alpha x} + c\alpha x_{ik}$,
$s_{\beta x} \leftarrow r_{\beta x} + c\beta x_{ik}$,
$s_{\rho x} \leftarrow r_{\rho x} + c\rho x_{ik}$,
$s_{\eta x} \leftarrow r_{\eta x} + c\eta x_{ik}$,

- Output group signature on message M:
$\sigma \leftarrow (t, k, T_1, \ldots, T_7, c, s_\alpha, s_\beta, s_\rho, s_\eta, s_x, s_{\alpha x}, s_{\beta x}, s_{\rho x}, s_{\eta x})$.

Signature verification $\mathsf{GVerify}(gpk, \bar{t}, M, \sigma)$: On input group public key gpk, current date $\bar{t}$, and the signature σ on message M, this algorithm verifies the validity of the signature and ensures that σ is not generated by a revoked user. It verifies the signature in the following steps.

- If $\bar{t} > t$, output $\perp$.
- $\{t_j\}_{j\in[1,l]} \leftarrow 0\text{-}\mathsf{ENC}(t)$.
- Recompute $R'_1, R'_2, R'_3, R'_4, R'_5, R'_6, R'_7, R'_8, R'_9, R'_{10}$ and R'_{11} as follows

$R'_1 \leftarrow u^{s_\alpha} T_1^{-c}$,
$R'_2 \leftarrow v^{s_\beta} T_2^{-c}$,
$R'_3 \leftarrow h^{s_\alpha + s_\beta} T_3^{-c}$,
$R'_4 \leftarrow e(T_4, g)^{s_x} e(g_1, w)^{-s_\alpha t_k} e(g_1, g)^{-s_{\alpha x}} e(g_2, w)^{-s_\beta t_k}$
$\cdot\, e(g_2, g)^{-s_{\beta x}} e(g, w)^{-s_\eta t_k} e(g, g)^{-s_{\eta x}}$,
$\cdot\, (e(g,g)/e(T_4, w^{t_k}))^{-c}$,
$R'_5 \leftarrow g^{s_\rho} T_5^{-c}$,
$R'_6 \leftarrow e(y, H_1(M))^{s_\rho} e(g,g)^{-s_\eta} T_7^{-c}$,
$R'_7 \leftarrow T_1^{s_x} u^{-s_{\alpha x}}$,
$R'_8 \leftarrow T_2^{s_x} v^{-s_{\beta x}}$,
$R'_9 \leftarrow T_5^{s_x} g^{-s_{\rho x}}$,
$R'_{10} \leftarrow T_6^{s_x} e(y, H_1(M))^{-s_{\rho x}} e(g,g)^{s_{\eta x}}$.
$R'_{11} \leftarrow e(T_7, g)^{s_x} e(f,g)^{-s_{\alpha x}} e(g,g)^{-c}$

- Verify whether the equation
$c \stackrel{?}{=} H_2(t, M, T_1, \ldots, T_7, R'_1, \ldots, R'_{11})$
holds. If the equation holds, the algorithm outputs 1, otherwise outputs $\perp$.

Batch verification $\mathsf{BVerify}(gpk, \bar{t}, (M_1, \ldots, M_\eta), (\sigma_1, \ldots, \sigma_\eta))$: Computing R'_4, R'_{11} are the most expensive part of the verification algorithm. However, we need to increase the signature size by six elements $(R_4, R_7, \ldots, R_{11})$ to accelerate the verification procedure. Let $\sigma_j \leftarrow (t_j, k_j, T_{j,1}, \ldots, T_{j,7}, R_{j,4}, R_{j,7}, \ldots, R_{j,11}, c_j, s_{j,\alpha}, s_{j,\beta}, s_{j,\rho}, s_{j,\eta}, s_{j,x}, s_{j,\alpha x}, s_{j,\beta x}, s_{j,\rho x}, s_{j,\eta x})$ be the new j^{th} signature on the message M_j for $j \in [1, \eta]$. Now we define a batch verifier where the main goal is to minimize the number of pairing calculation. For each $j \in [1,\eta]$, compute only $(R'_{j,1}, R'_{j,2}, R'_{j,3}, R'_{j,5}, R'_{j,6})$ following the above mentioned way. For each $j \in [1,\eta]$, check that $c_j \stackrel{?}{=} H_2(t_j, k_j, T_{j,1}, \ldots, T_{j,7}, R_{j,1}, \ldots, R_{j,11})$. Then check the following pairing based equation:

$\prod_{j=1}^{\eta} R_{j,4}^{\delta_j} \stackrel{?}{=} e(\prod_{j=1}^{\eta} (T_{j,4}^{s_{j,x}} \cdot g_1^{-s_{j,\alpha x}} \cdot g_2^{-s_{j,\beta x}} \cdot g^{-s_{j,\eta x} - c_j})^{\delta_j}, g)$
$\cdot e(\prod_{j=1}^{\eta} (g_1^{-s_{j,\alpha t_k}} \cdot g_2^{-s_{j,\beta t_k}} \cdot g^{-s_{j,\eta t_k}} \cdot T_4^{-c_j t_k})^{\delta_j}, w)$

$\prod_{j=1}^{\eta} R_{j,11}^{\delta_j} \stackrel{?}{=} e(\prod_{j=1}^{\eta} (T_{j,7}^{s_{j,x}} \cdot f^{-s_{j,\alpha x}} \cdot g^{-c_j})^{\delta_j}, g)$

and

$1_{\mathbb{G}} \stackrel{?}{=} (R_{j,7} R_{j,8} R_{j,9} R_{j,10})^{-\delta_j} (T_{j,1} T_{j,2} T_{j,5} T_{j,6})^{-\delta_j s_{j,x}}$
$u^{-s_{j,\alpha x}} v^{-s_{j,\beta x}} g^{-s_{j,\rho x}} e(y_j, H_1(M_j))^{-s_{j,\rho x}} e(g,g)^{s_{j,\eta x}}$

where $(\delta_1, \ldots, \delta_\eta) \in \mathbb{Z}_p$ is a random vector of l_b bit. Accept if and only if all checks pass successfully.

Message attestation $\mathsf{TAtd}(gpk, ak, M)$: Given attestation $ak = \zeta$, and M, the algorithm generates a token t_M on M such that $t_M \leftarrow H_1(M)^\zeta$ and outputs t_M. This token can be used together with $\mathsf{Open}(gpk, ok, M, \sigma, t_M)$ algorithm to extract signer's identity.

Attested tracing$\mathsf{Open}(gpk, aok, M, \sigma, t_M)$: Given gpk, aok, M, σ, and a token t_M on message M, this algorithm first verifies the signature using the algorithm $\mathsf{GVerify}$. If the signature is invalid, the algorithm outputs $\perp$. Otherwise, it searches i in the registration table *reg*$_1[i]$ to find $e(A_{ij}, g) \leftarrow$*reg*$[i]$ that satisfies the following equation $e(\frac{T_4}{T_1^{\zeta_1} T_2^{\zeta_2} T_3^{\zeta_3}}, g) \cdot \frac{T_6}{e(T_5, t_M)} \stackrel{?}{=} e(A_{ij}, g)$. The algorithm outputs i if it exists, otherwise outputs $\perp$.

Direct tracing $\mathsf{DTrace}(gpk, dok, M, \sigma)$: By accessing the registration table *reg*$_2[i]$, this algorithm can revoke the signer's identity i of a valid signature σ on message M. Note that unlike **Attested tracing** $(\mathsf{Open}(gpk, ok, M, \sigma, t_M))$, this algorithm use no *token* in order to trace the identity of the signer. It extracts the part of the member group secret key $e(T_7/T_1^\ell, g) \stackrel{?}{=} e(g,g)^{x_{ij}}$ and match the record in the *reg*$_2[i]$.

Managing Linkability $\mathsf{SignLink}((\sigma, M), (\sigma', M'), lk)$: Given two message (M, M') and their corresponding signatures (σ, σ'), and linking key $lk \leftarrow h^\ell$, this algorithm tries to

find links among signatures whether they are generated from the same signer i. It first verifies the signatures' validity by using the algorithm GVerify. Then it checks $e(T_7/T_7', h) \stackrel{?}{=} e(T_1/T_1', lk)$. It returns 1 if successful, otherwise outputs $\perp$. We assume that x_i is picked uniformly at random so that $x_i \neq x_j$ for any i, j.

Revocation Revoke(gpk, gsk_i, A'', w''): Revocation would be accomplished in two ways:

- Verifier-Local Revocation (VLR): Adopting 0/1 *encoding system* enables the group manager (Issuer) to embed the key expiration date in each signing key. It ensures that the signature will pass the verification algorithm GVerify$(gpk, \bar{t}, M, \sigma)$ only if the *key expiration* date is larger than the *signature expiration* date. Although proposed scheme is not completely satisfying the requirement of traditional VLR scheme where verifier holds a list of special information called Revocation List (RL) for each revoked signer. But it partially helps the verifier to revoke the expired signers (vehicles) locally.

- Re-keying the signature scheme: In Re-key based revocation solution, the issuer updates its public key gpk, and hence, the execution of signing and verification algorithms are affected subsequently. At each update of the key, a former signer would become no longer a legitimate signer unless it updates its credentials it holds. The Re-key revocation process is done in a fixed time interval. The advantage of this mechanism is that each signer knows when the rekey process will take place. The drawback is that no legitimate signer will be revoked within this interval. Note that, this interval could be flexible, that is, rekeying will happen when the group shrinks with some members leaving. But the later choice is opposite to the former one and also inefficient. The length of the interval is then dependent on applications. During GKgen$(1^\lambda, 1^l, 1^n)$ algorithm execution, Issuer generates the credential $gsk_i \leftarrow (A, x, d)$ for each signer. To update group public key gpk and credential gsk_i for each currently legitimate signer i, the issuer first choose its private key by deriving a new value $\gamma'' \in \mathbb{Z}_p$. For each currently legitimate signer, the issuer updates the credential element A with
$$A'' \leftarrow g^{1/(\gamma'' d_j + x_j)_{j \in [1,l]}}$$
The issuer makes A'' available to corresponding signer (new credential $gsk_i \leftarrow (A'', x, d)$) and publishes $w'' \leftarrow g^{\gamma''}$ to replace w in its public key gpk. The signer may optionally check whether the new gsk_i is associated to the gpk by
$$e(A'', w^d g^x) \stackrel{?}{=} e(g, g)$$

Theorem 1. Our group signature scheme is correct.

Theorem 2. If the decisional Diffie-Hellman assumption holds in $\mathbb{G}$, our construction with time-bound keys has anonymity in the random oracle model.

Theorem 3. If the discrete logarithm assumption holds, our construction has linkability in the random oracle model.

Theorem 4. If the decision bilinear Diffie-Hellman assumption holds, our construction has attested opener anonymity in the random oracle model.

Theorem 5. If the decision linear assumption holds, our construction has admitter anonymity in the random oracle model.

Theorem 6. If the q-strong Diffie-Hellman assumption holds, our construction has traceability in the random oracle model.

Proof: Proof of the *Theorem*[1-6] has been deferred for the full version of the paper.

V. Security and Performance comparison

We compare our GS scheme based on BBS GS [23] with the other related VANET GS proposals such as Hwang *et al.*[28], Qin *et al.* [32], Mamun *et al.*[10], Zhang *et al.*[29], Malina *et al.*[35], Zhang *et al.*[3]. Table I. shows a comparative study on the aforementioned schemes.

We provide construction for more stringent security notions (CCA anonymity). In compare to the GS scheme [15], we introduce only one additional element (in $\mathbb{G}_1$) in the basic signature to satisfy two additional properties (linkability, direct opening). Moreover, unlike other proposals, we refer hybrid revocation (limited VLR + Rekeying) system. Our VLR solution works only with signer's expiration date (constant verification cost). It rules out expensive revocation check (checking revoked member list) for each signature verification. It is worth mentioning that the verification cost in [35], [29] (as authors claimed) does not reflect the literal cost. It actually depends on the size of revoked member list (RList).

For signature length, we consider the MNT curve with $\mathbb{G}_1 = 161$ bits, $\mathbb{G}_T = 483$ bits and $\mathbb{Z}_p = 160$ bits. In general, bilinear pairing T_p is the most expensive operation (10 $\times$ exponentiation operation T_e) while one point multiplication T_m is the least. Our proposal achieves the maximum functionality of the GS with optimum cost (signature length and verification). Our efficient batch verification cost includes $(4T_p + 14nT_e)$ for n signatures. Note that, we need to increase the signature size by 6 elements ($3\mathbb{G}_1$, $3\mathbb{G}_T$) for batch verification.

We implement our scheme on an Intel Core i3 model CPU @2.43 GHz using the PBC library [37] running on top of Gnu GMP [36] on Ubuntu 12.10. They use a supersingular curve (order is a Solinas prime). The processing time for one bi-linear operation T_p, a single exponentiation T_e, and one point multiplication are respectively 3.1 *ms*, .4 *ms*, and .3 *ms*. The verification of a single signature takes approximately 21 *ms* (considering some pre-computation like $e(g, g), e(g, w), e(f, g)$ etc.) that is very close to Mamun et al. scheme (19 *ms*) in [10]. However, for batch verification, it will be much more efficient on average.

VI. Conclusion

In this paper, we have presented a CCA-secure short group signature solution considering hybrid revocability, linkability and message-depend opening for an application-friendly VANET environment. We focus on relaxed privacy that can be efficiently used for a hierarchical VANET architecture.

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] Zhang, Lei, Qianhong Wu, Agusti Solanas, and Josep Domingo-Ferrer. A scalable robust authentication protocol for secure vehicular communications. Vehicular Technology, IEEE Transactions on 59, no. 4 (2010): 1606-1617.

[4] Gerlach, M., Festag, A., Leinmuller, T., Goldacker, G., Harsch, C. Security architecture for vehicular communication. In: The 5th International Workshop on Intelligent Transportation, 2007.

[5] Chen, Liqun, and Jiangtao Li. Revocation of direct anonymous attestation. In Trusted Systems, pp. 128-147. Springer Berlin Heidelberg, 2011.

[6] Zhang, L., Wu, Q., Solanas, A., Domingo-Ferrer, J. A scalable robust authentication protocol for secure vehicular communications. IEEE Transactions on Vehicular Technology 59(4), 16061617, 2010.

[7] Lin, X., Sun, X., Han Ho, P., Shen, X. GSIS: A secure and privacy preserving protocol for vehicular communications. IEEE Transactions on Vehicular Technology 56, 34423456, 2007.

[8] Chim, T.W., Yiu, S.M., Hui, L.C.K., Li, V.O.K. SPECS: Secure and privacy enhancing communications schemes for VANETs. Ad Hoc Networks 9(2), 189-203, 2011.

[9] Lin, Hsiao-Ying, and Wen-Guey Tzeng. An efficient solution to the millionaires problem based on homomorphic encryption. In Applied Cryptography and Network Security, pp. 456-466. Springer Berlin Heidelberg, 2005.

[10] MSI Mamun, Atsuko Miyaji. An efficient batch verification system for large scale VANET. Intl. J. of Security and Communication Networks (SCN), Wiley Publication DOI: 10.1002/sec.980, 2014.

[11] Bo Qin, Qianhong Wu, Josep Domingo-Ferrer, and Lei Zhang, Preserving Security and Privacy in Large-Scale VANETs, ICICS 2011, LNCS 7043, pp. 121-135, 2011.

[12] Zhang, C., Lu, R., Lin, X., Ho, P.H., Shen, X. An efficient identity-based batch verification scheme for vehicular sensor networks. In: INFOCOM, pp. 246-250. IEEE, 2008.

[13] Chu, Cheng-Kang, Joseph K. Liu, Xinyi Huang, and Jianying Zhou. Verifier-local revocation group signatures with time-bound keys. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 26-27. ACM, 2012.

[14] Guomin Yang, Qiong Huang, Duncan S. Wong, and Xiaotie Deng. Universal authentication protocols for anonymous wireless communications.IEEE Transactions on Wireless Communications ,9(1):168174, 2010.

[15] Ohara, K., Sakai, Y., Emura, K., Hanaoka, G. (2013, May). A group signature scheme with unbounded message-dependent opening. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (pp. 517-522). ACM.

[16] Ferrara, A. L., Green, M., Hohenberger, S., Pedersen, M. (2009). Practical short signature batch verification. In Topics in CryptologyCT-RSA 2009 (pp. 309-324). Springer Berlin Heidelberg.

[17] P. Papadimitratos, L. Buttyan, J. Hubaux, F. Kargl, A. Kung, M. Raya. Architecture for Secure and Private Vehicular Communications. In: Intl. Conference on ITS Telecomm. , pp. 16 (2007)

[18] Heen, O., Guette, G., Genet, T. On the unobservability of a trust relation in mobile ad hoc networks. In Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks (pp. 1-11). Springer Berlin Heidelberg, 2009.

[19] Buttyan, L., Holczer, T., Weimerskirch, A., Whyte, W. SLOW: A practical pseudonym changing scheme for location privacy in vanets. In Vehicular Networking Conference (VNC),(pp. 1-8). IEEE 2009.

[20] Mamun, M. S. I., Miyaji, A. An Optimized Signature Verification System for Vehicle Ad Hoc NETwork. The 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), pp.1-8, 2012.

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

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

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

[24] 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.

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

[26] Wei, Lingbo, and Jianwei Liu. Shorter verifier-local revocation group signature with backward unlinkability. In Pairing-Based Cryptography-Pairing 2010, pp. 136-146. Springer Berlin Heidelberg, 2010.

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

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

[29] 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.

[30] 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.

[31] 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.

[32] Bo Qin, Qianhong Wu, Josep Domingo-Ferrer, and Lei Zhang, Preserving Security and Privacy in Large-Scale VANETs, ICICS 2011, LNCS 7043, pp. 121-135, 2011

[33] 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.

[34] 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.

[35] Malina, Lukas, et al. Short-Term linkable group signatures with categorized batch verification. Foundations and Practice of Security. Springer Berlin Heidelberg, 2013.

[36] The GNU Multiple Precision Arithmetic Library.
web: http://gmplib.org/

[37] The Pairing based Cryptography(PBC)Library.
web: http://crypto.stanford.edu/pbc/