Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 473151, 6 pages
http://dx.doi.org/10.1155/2014/473151

*Research Article*

# A Collaboratively Hidden Location Privacy Scheme for VANETs

**Ying Mei,[1,2] Guozhou Jiang,[2] Wei Zhang,[3] and Yongquan Cui[1]**

[1] *School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China*
[2] *College of Educational Information and Technology, Hubei Normal University, Huangshi 435002, China*
[3] *School of Computer, Central China Normal University, Wuhan 430079, China*

Correspondence should be addressed to Yongquan Cui; yqcui1977@hust.edu.cn

Received 15 December 2013; Revised 15 February 2014; Accepted 26 February 2014; Published 24 March 2014

Academic Editor: Jiun-Long Huang



Communication messages in vehicular ad hoc networks (VANETs) can be used to locate and track vehicles, and this can lead to threats on location privacy of vehicle users. In this paper, we address the problem of privacy and liability in VANETs. We propose a scheme that provides location privacy by utilizing a variant of ring signature. It allows a vehicle to form a ring arbitrarily with nearby vehicles and sign its messages anonymously, so that it can hide itself in the surrounding vehicles. When solving a dispute, the real signer will be responsible for what it has signed as the anonymity is revocable by the authority.

## 1. Introduction

The continuing advances of vehicular ad hoc networks (VANETs) have elevated the intelligent transportation systems (ITSs) to higher levels. Although VANETs can benefit us with rich applications to improve safety, efficiency, and convenience in transportation, it cannot be widely accepted by the public if a VANET discloses any privacy information of users, for example, location privacy. It cannot widely be accepted by the public. Therefore, to provide guaranteed location privacy to users is a prerequisite for the wide acceptance of VANETs to the public.

Multiple solutions have been proposed to address this issue.

(1) Anonymous certificates [1, 2]. It uses a list of anonymous certificates for message authentication; every time when a vehicle wants to communicate with the network it randomly chooses one of the available certificates to sign a particular message and then discards it. The ID management authority stores all the anonymous certificates for each vehicle in its administrative region; once a malicious node is detected, the authority has to exhaustively search in a large database to find the ID related to the misbehaving anonymous public key. Besides, if a node needs to be revoked, all its anonymous certificates have to be included in the CRL, which will then grow very fast.

(2) Group signatures [3]. The vehicles hide in a group and use the group's public key to do sign operation on behalf of the group, but there are also some flaws: (1) before the update operation of group, including new nodes join and old nodes exit, the program should initialize the entire system and change keys of all the members even the group's public key, which will take up a lot of system resources; (2) the length of group public key and group signature depend on the group size.

(3) Pseudonyms [4–6]. Pseudonym is the identifier of a vehicle entity, which can be pregenerated for permanent use or generated temporarily. Pseudonymous authentication is widely accepted in the VANET community. To achieve location privacy in all pseudonyms schemes, a popular approach that is recommended in VANETs is that vehicles periodically change their pseudonyms when they broadcast safety messages. Although frequent pseudonym changing provides a promising solution for location privacy in VANETs, this solution may become invalid if the pseudonyms are changed in an improper time or location; such a solution may become invalid. There are

two main approaches to change pseudonyms. One is silent period [7, 8]. The silent period schemes make a vehicle stop broadcasting for a random period to provide anonymity. They can provide good anonymity to a vehicle, but potentially at the cost of safety and liability. Another is mix zone [9, 10]. The mix-zone schemes make vehicles change their pseudonyms in the mix zone to obfuscate the relation between events of entering and exiting from a mix zone. They are appealing but rely on the predetermined locations and thus lack flexibility.

(4) Ring signatures [11, 12] are representative proposals. The two main properties of ring signature are spontaneity and anonymity. Spontaneity allows the actual signer to create a signer group on the fly without taking the consent of the other possible signers to disseminate messages. Anonymity of a ring signature protects the actual signer in such a way that no one can identify who the actual signer is among the ring members. Compared with group signature, ring signature reduces a lot of updates, key agreement, and other expenses. Although this scheme can effectively meet the conditional privacy requirement, to the best of our knowledge, no scheme given a detailed description about how the traveling vehicle forms a same ring with nearby vehicles.

In this paper, inspirited by some proposed ideas, such as ring signature and mix zone, we present a collaboratively hidden location privacy scheme. In our scheme, we authenticate beacon messages by employing a ring signature scheme and explore some approaches to solve the ring formation problem in different situations. We proposed two approaches for ring formation in two different situations.

The rest of this paper is structured as follows. We start in Section 2 with describing VANET architecture, formalizing the problem and introducing associated cryptographic technologies. Section 3 details our proposed scheme. In Sections 4 and 5, we provide security and performance analysis. Last, we sum up our paper with a conclusion in Section 6.

## 2. Background

*2.1. VANET Architecture.* A typical VANET consists of vehicles which is equipped with an onboard unit (OBU), road side units (RSUs), and trusted authority (TA). As shown in Figure 1, the TA initializes the system parameters and provides registration services for vehicles. All the vehicles register with the TA before joining the VANET. Vehicles can communicate with each other directly forming a vehicle to vehicle communication (V2V) or communicate with fixed equipment next to the road, referred to as road side unit (RSU) forming a vehicle to infrastructure communication (V2I). Vehicles are involved in both safety applications and other applications like traffic managements and online services by using V2V and V2I communications. RSUs are physically connected to the VANET infrastructure by a wired network and are managed by the trusted authority such as

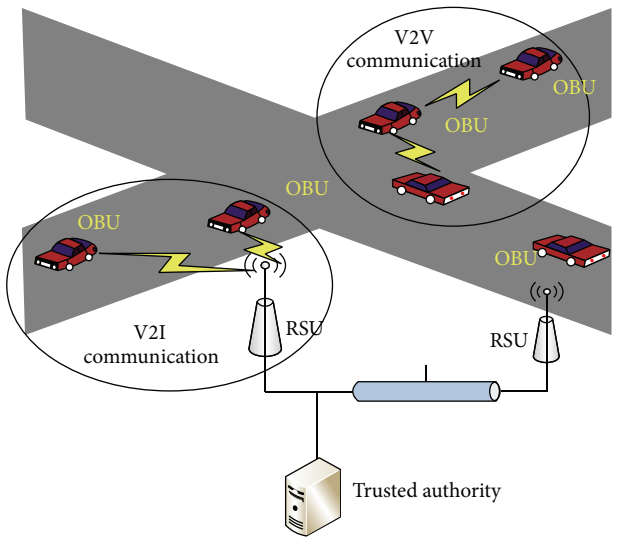


Figure 1: VANET architecture.

Department of Transportation. RSUs can broadcast some common messages such as the identity of revoked vehicle.

*2.2. Privacy Requires.* An eavesdropper, through the safety messages that are broadcasted by the OBU, can monitor the location information of a specific vehicle at all times. To resist the adversary's tracking and achieve location privacy in VANETs, the following requirements must be satisfied.

R.1 Each vehicle should not use a real identity to broadcast messages. Then, by concealing the real identity, the identity privacy can be achieved.

R.2 Each vehicle should also cut down the relation between the former and the latter locations.

R.3 Location privacy should be conditional in VANETs. If a broadcasted safety message is in dispute, the trusted authority (TA) can disclose the real identity.

*2.3. Bilinear Groups of Composite Order.* We review some general notions about bilinear maps and groups of composite order [13]. Consider two finite cyclic groups $G$ and $G_T$ of same order $n$, where $n = pq$ has a (hidden) factorization in two large primes; $p \neq q$ in which the respective group operation is efficiently computable and denoted multiplicatively. Assume the existence of an efficiently computable function $e : G \times G \to G_T$, with the following properties:

(i) (bilinearity) $\forall u, v \in G$, $\forall a, b \in Z_n$, and $e(u^a, v^b) = e(u, v)^{ab}$, where the product in the exponent is defined modulo $n$;

(ii) (nondegeneracy) $\exists g \in G$ such that $e(g, g)$ has order $n$ in $G_T$. In other words, $e(g, g)$ is a generator of $G_T$, whereas $g$ generates $G$.

If such a function can be computed efficiently, it is called a (symmetric) bilinear map or pairing, and the group $G$ is called a bilinear group. We denote by $G_p$ and $G_q$ the subgroups of $G$ of respective orders $p$ and $q$.

*2.4. Ring Signature.* Ring signatures were introduced by Rivest et al. [14], which enables the signer to keep anonymous in the ring, while allowing the real signer to form a ring arbitrarily without being controlled by any other part. Shacham and Waters ring signature can show our scheme is anonymous against full key exposure and unforgeable with respect to insider corruption [15]. Since it provides the spontaneity, it is very suitable for our privacy requirements in VANETs.

*2.5. NIZK Proof of Plaintext Being Zero or One.* Groth et al. proposed a noninteractive zero-knowledge (NIZK) protocols in [16] as follows.

*Statement.* The statement is an element $c \in G$. The claim is that there exists a pair $(m, w) \in Z^2$ so $m \in \{0, 1\}$ and $c = g^m h^w$.

*Proof.* Input $(c, (m, w))$

(1) Check $c \in G$, $m \in \{0, 1\}$, and $c = g^m h^w$. Return failure if check fails.

(2) $r \leftarrow Z_n^*$, $\pi_1 = h^r$, $\pi_2 = (g^{2m-1} h^w)^{wr^{-1}}$, and $\pi_3 = g^r$.

(3) Return $\pi = (\pi_1, \pi_2, \pi_3)$.

Verification. Input $(c, \pi)$

(1) Check $c \in G$, $\pi \in G^3$.

(2) Check $e(c, cg^{-1}) = e(\pi_1, \pi_2)$ and $e(\pi_1, g) = e(h, \pi_3)$.

(3) Return 1 if both checks pass, else return 0. □

## 3. Proposed Location Privacy Scheme

In this section we detail our proposed scheme. Ring signature provides a good anonymity and spontaneity, and it is ideally suitable for message authentication in VANETs. Spontaneity allows the actual signer to form a ring of members arbitrarily without collaboration of any of those ring members, provided that the actual signer is also in the ring, and this leaks some identity information to the adversaries. The signed messages can be linked to a specific vehicle if the vehicle signs messages with a distinguishable ring when it is traveling on the road. If the vehicles traveling on the road can sense the presence of surrounding vehicles and form a ring with them and the vehicles sign messages with the ring containing the respective pks, then they can successfully hide themselves in the vehicle group, which can effectively cut off the linkability between the messages and the vehicles. However, anonymity of a ring signature protects the actual signer in such a way that no one can identify who the actual signer is among the ring members.

In our scheme, we authenticate beacon messages by using ring signature technique. It is an intractable problem, that is, how to find the pks of the nearby vehicles and form a common ring with them. To address this issue we design a Signed Timestamps Message (STM) by which a vehicle signs a timestamp with a ring that just contains the only pk of the signer. Although this type of messages exposes the user's identity, it takes place in a transient time, and it can form a ring immediately with its neighbors, so this type of messages cannot thwart user's privacy. We propose two approaches for broadcasting STM in a suitable location or time. They are centralized and distributed.

With the centralized approach, inspirited by scheme of changing pseudonym at social spots [17], vehicles broadcast their STM together in predetermined social spots. The social spots in the urban area refer to the places where several vehicles gather, for example, a road intersection when the traffic light is red or a free parking lot near the shopping mall. Because social spots usually hold many vehicles, if all vehicles indistinguishably broadcast messages using same ring in the spots, the social spots naturally become mix zones. In this case, each vehicle broadcasts a STM when vehicles enter the social spots almost at the same time slot. The nearby RSU collects pks and sorts them by time, then divides them into rings of size $k$ ($k$ is the size of anonymity set described as [17]), and then broadcasts them to all vehicles. Each vehicle will sign messages with the ring containing his pks.

With the distributed approach, no the help of RSUs, vehicles can dynamically choose time and location to broadcast STM by the coordination among neighboring vehicles in the case of nonsocial spots. Inspirited by CPN scheme [18], we design a collaboratively hidden approach. We first give an assumption and a definition. All vehicles are equipped with GPS devices and their broadcasts are synchronous with the same period, called time slot. We give a general framework of cooperation on broadcast STM based on a trigger. In which a flag is inserted into beacons to indicate if a vehicle is eligible to broadcast STM. We can think that the anonymity set of a vehicle mainly depends on the number of neighbors signing beacon with the same ring as it; we take this number as a trigger. When vehicles are traveling on the road, each vehicle estimates the number of neighbors that sign with same ring by analyzing the received message; if this number is less than the size of the anonymity set, it will send out a STM in next time slot. The nearby vehicles extract pks from received STM and form a common ring, and then the vehicle included in this ring will sign beacon with this ring. So it can hide itself in the neighbors.

Our scheme includes five phases, which are system setup, registration, signing, and verifying, as well as tracing and revoking and two algorithms: *form-in-sp()* and *form-in-nsp()* as described below. The notation used throughout this paper is listed in notations and their brief descriptions section.

*3.1. System Setup.* The TA first constructs a group G of composite order $n = pq$ as described in Section 2 above. It then chooses two exponents $a, b \in_R Z_n$ and sets $A = g^a$, $B = g^b$, and $\widehat{A} = h^a$. Let $H : \{0, 1\}^* \rightarrow \{0, 1\}^k$ be a collision-resistant hash function. Then the TA picks Waters hash generators $u, u_1, u_2, \ldots, u_k \in_R G$. The TA publishes a common reference string which includes a description of the group $G$ and the collision-resistant hash function $H$, along with $(A, B, \widehat{A})$ and $(u, u_1, \ldots, u_k)$.

*3.2. Registration.* In our system, all members (including OBUs and RSUs) register with the TA before joining the VANET. They can use the public parameters published by the

TA to register to the TA and to generate their own keys. A member chooses a random exponent $i \in_R Z_n$; set $\mathrm{pk}_i = g^i \in G$ and send it to the TA. Then the TA verifies its identity $\mathrm{ID}_i$ and bands it with its $\mathrm{pk}_i$. The user keeps $\mathrm{sk}_i = A^i \in G$ secret as its private key.

*3.3. Signing.* A vehicle can broadcast beacon messages signed with a ring $R$. It takes a message $M \in \{0,1\}^*$ as an input and chooses a ring $R$ of the public keys (no key may appear twice in $R$, and $R$ must include pks), and a key pair $(pk, sk) \in G^2$. Compute $(m_1, \ldots, m_k) \leftarrow H(M, R)$. Let $l = |R|$; parse the elements of $R$ as $v_i \in G$, $1 \le i \le l$. Let $i^*$ be the index such that $v_{i^*} = \mathrm{pk}$. Define $\{f_i\}_{i=1}^l$ as

$$f_i = \begin{cases} 1, & \text{if } i = i^*, \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

Now for each $i$, $1 \le i \le l$, choose a random exponent $t_i \in_R Z_n$ and set $C_i = (v_i/B)^{f_i} h^{t_i}$ and $\pi_i = ((v_i/B)^{2f_i - 1} h^{t_i})^{t_i}$. Let $t = \Sigma_{i=1}^l t_i$, choose $r \in_R Z_n$, and compute $S_1 = \mathrm{sk} \cdot (u' \prod_{j=1}^k u_j^{m_j}) \cdot \widehat{A}^t$ and $S_2 = g^r$. The signature is output as $\sigma = ((S_1, S_2), \{(C_i, \pi_i)\}_{i=1}^l) \in G^{2l+2}$.

The RSU signs its messages by ring signature as described above. Because it is considered as a public infrastructure, its identity can be public, and its signing ring can just contain the only pks of itself.

*3.4. Verifying.* Compute $(m_1, \ldots, m_k) \leftarrow H(M, R)$. Let $l = |R|$; parse the elements of $R$ as $v_i \in G$, $1 \le i \le l$. Verify that no element is repeated in $R$ and reject otherwise. Parse the signature $\sigma$ as $\sigma = ((S_1, S_2), \{(C_i, \pi_i)\}_{i=1}^l) \in G^{2l+2}$ (if this parse fails, reject). Check first that whether the proofs $\{\pi_i\}$ are valid: for each $i$, $1 \le i \le l$, if $e(C_i, C_i/(v_i/B)) \stackrel{?}{=} e(h, \pi_i)$ holds. If any of the proofs is invalid, reject. Otherwise, set $C = \prod_{i=1}^l C_i$. Accept if the following equation is satisfied: $e(A, BC) = e(S_1, g) \cdot e(S_2^{-1}, u' \prod_{j=1}^k u_j^{m_j})$.

*3.5. Tracing and Revoking.* When being in a dispute, given the signed message $(M|R|\sigma)$, the TA can trace the identity of the real signer by using its secret parameter $q$. The TA verifies the signature and parses the signature $\sigma$ as $\sigma = ((S_1, S_2), \{(C_i, \pi_i)\}_{i=1}^l) \in G^{2l+2}$ (if this parsing fails, the TA reject), then it tests $(C_i)^q$, $1 \le i \le l$, and finds a $i^*$ making $(C_i)^q \ne g^0$. Then we can decide whether the $i^*$th element of $R$ is the real signer.

The identity of the misbehavior must be revoked. The TA can broadcast the revoked pks through RSUs. When the vehicles receive the revoked pks, they store the pks in the RCL.

*3.6. 2 Ring Formation Algorithms.* In this section, we introduce two ring formation algorithms.

In social spots such as a road intersection when the traffic light is red or a free parking lot near the shopping mall, the social spots naturally become mix zones. Because the social spots usually hold many vehicles, they can negotiate common ring with nearby vehicles with Algorithm form-in-sp($k$).

*Algorithm 1* (form-in-sp($k$)). Consider forming a ring with nearby vehicles in social spots.

When a vehicle enters social spots, it sends out a STM. RSU receives the messages and verifies the message. If it is a valid message, the RSU accepts and stores the pks into an array. Assuming that the size of predefined anonymity set is $K$, the RSU will send out a $K + 1$ sizes pks set $(\mathrm{pk}_1, \mathrm{pk}_2, \ldots, \mathrm{pk}_K, \mathrm{pk}_{\mathrm{RSU}})$ when it accumulates $K$ pks. Vehicles receiving messages from the RSU check whether it is included in this set. If true, it verifies the message; if the message is valid, it will sign messages with this $R$ (delete RSU's pks). Otherwise, it discards it.

In the case of nonsocial spots, because the cost of deploying the RSUs is high, thus likely only some of the roads will be fully covered especially at the initial deployment stage of VANETs, and the vehicles are mobile with high speed. Therefore, the centralized solution is not feasible in this case; they form a common ring through the collaboration between nearby vehicles. They broadcast STM at a same time slot and form a ring as follows:

*Algorithm 2* (form-in-nsp($k$)). Consider forming a ring with near vehicle in nonsocial spots.

To implement the cooperation, we introduce a "Readyflag" bit which is inserted into beacons. A vehicle's "Readyflag" has 2 meanings: (i) it meets the trigger and (ii) it sends out STM in the next slot. Upon receiving beacons from neighbors in the last slot, a vehicle first checks its own "Readyflag." If "Readyflag" is 1, it sends out STM and sets its "Readyflag" to 0. Otherwise, the vehicle checks whether it receives a beacon in which "Readyflag" is 1. If so, it sends out STM. If the vehicle does not meet the former two conditions, it checks if it meets the trigger. If so, it sets its "Readyflag" to 1, which means it will send STM in the next slot. Vehicles traveling on the road extract the pks from STM and form a common ring with neighbors.

## 4. Security Analysis

In this section, we make a security analysis of our scheme from following aspects, anonymity and unforgeability, unlinkability, and traceability.

**Lemma 3.** *For an originator of a valid message, its identity is kept anonymous.*

*Proof (sketch).* If there exists an attacker $\mathscr{A}$, which can successfully break the anonymity of the proposed scheme, then we can construct an efficient algorithm $\mathscr{B}$, which can make use of attacker $\mathscr{A}$ to break the underlying ring signature [15]. Then we could use $\mathscr{B}$, with $\mathscr{A}$ as a subroutine to solve Subgroup Hiding (SGH) assumption, but the assumption is that the subgroup decision problem is hard. □

**Lemma 4.** *An attacker cannot forge the signature of a message to cheat other vehicles and make sure that it can pass the verification of the honest vehicle.*

Table 1: Comparison of three schemes.

| Scheme | S.O.O | Building block | S.O.O | R.F. |
|---|---|---|---|---|
| Scheme [11] | $m+1$ | Provably secure without random oracle | $2l+2$ | No |
| Scheme [12] | $m+1$ | Provably secure in the random oracle | $2l+1$ | No |
| Our scheme | $m+1$ | Provably secure without random oracle | $2k+2$ | Yes |

S.O.O: storage of OBU.
S.O.S: size of signature.
R.F: ring formation.

*Proof (sketch).* If there exists an attacker $\mathcal{A}$, which can successfully forge the signature of message, then we can construct an efficient algorithm $\mathcal{B}$, which can make use of attacker $\mathcal{A}$ to break the unforgeability of the underlying ring signature [15]. Thus we obtain from a ring signature forging adversary a break of either the collision resistance of H or the computational Diffie-Hellman (CDH) hardness of $G_p$. □

**Lemma 5.** *Our scheme provides long-term location privacy.*

*Proof.* First, because of the anonymity of the underlying ring signature, given a valid ring signature $\sigma$ of some message, it is computationally difficult to identify the actual signer for any participant in the system except the TA. But it is very easy to link a message to a vehicle when just one car driving on the road or vehicles sign message with distinguished ring. In our scheme, a vehicle forms a ring with nearby vehicles and signs message with the same ring. So the attacker just only guesses that the real signer comes from a ring with probability $1/|R|$ and cannot link a message with a special vehicle. They reform a new ring when they enter the social spots or meet the trigger. This can confuse the linkability of messages and guarantee the long-term location privacy of the vehicles. □

**Lemma 6.** *If a vehicle has malicious behavior, the trusted third party can reveal the real identity of the vehicle to trace its liability.*

*Proof.* By the perfect binding property of the underlying NIZK technique, a signature can be traced to a specific user. When being in a dispute, a valid signature $(M, R, \sigma)$ of the message $M$ is given to the TA, and the TA has the tracing key $\mathrm{TK} = q$. The pks of the real identity must be included in the ring $R$, and the TA can recover it by test $(C_i)^q$ as described in Section 3.5. □

## 5. Performance Evaluation

Comparing our scheme with two previously proposed ring signature based schemes [11, 12], only our scheme addresses the issue of ring formation, although the ring formation algorithm increases the computational overhead of vehicles, but it can provide the unlinkability of messages sent by vehicles. Our scheme and scheme [11] use the ring signature [15] as building block that is provably secure without random oracles, but the building block of scheme [12] is provably secure in the oracle random model. The main communication overhead is coming from the periodically broadcast beacons messages. In scheme [11], the signatures of the messages are of size $2l+2$ group elements for $l$ members in a ring, but the size of the group did not give a clear explanation. In scheme [12], the signatures of the messages are of size $2l+1$ group elements for $l$ members in a ring; the size of the group did not give a clear explanation too. In our scheme, the signatures of the messages are of size $2k+2$; the size of ring is $k$ ($k$ is the size of anonymity set). About the storage cost in vehicles, each OBU stores one private key issued by the trusted party and m revoked public keys in the revocation list in all three schemes. Let each key (with its certificate) occupy one storage unit; it is $m+1$ units. We give a summarization about the performance comparison of three schemes in Table 1.

## 6. Conclusion

In this paper, we have proposed an effective scheme for location privacy in VANETs. All messages in our system can be authenticated using a ring signature scheme, and the underlying ring signature can provide good properties of anonymity and spontaneity. For the problem about how to form a ring with nearby vehicles, we proposed two approaches for different situations. The centralized approach needs the help of infrastructure. The distributed approach is relatively flexible and is suitable to be implemented in the nonsocial spots situation because a vehicle with the scheme can decide the time and location to send out STM. Making simulation in NS-2 and exploring how to improve the efficiency of our scheme are our future work.

## Notations and Their Brief Descriptions

| | |
|---|---|
| $G, G_T$: | Two multiplicative cyclic group of order $n = pq$ |
| $G_q$: | The cyclic order-$q$ subgroup of $G$ |
| $q$: | The tracing key of TA |
| $g$: | The generator of $G$ |
| $h$: | The generator of $G_q$ |
| $e : G \times G \to G_T$: | An efficiently computable bilinear map |
| $a, b, A, B, \widehat{A}$: | $a, b \in_R Z_n$; $A = g^a$; $B = g^b$; $\widehat{A} = h^a$ |
| $(u, u_1, \ldots, u_k)$: | Waters hash generators, $u, u_1, \ldots, u_k \in_R G$ |
| $\mathrm{ID}_i$: | The real identity of the vehicle $V_i$ |
| $\mathrm{pk}_i$: | The public key of the vehicle $V_i$, $\mathrm{pk}_i = g^i \in G$ |

$sk_i$: The private key of the vehicle $V_i$, $sk_i = A^i \in G$

$\sigma$: The message signature

$H: \{0,1\}^* \rightarrow \{0,1\}^k$: A collision-resistant hash function.

## Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

## References


[1] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[2] C. Laurendeau and M. Barbeau, "Secure anonymous broadcasting in vehicular networks," in *Proceedings of the 32nd IEEE Conference on Local Computer Networks (LCN '07)*, pp. 661–668, October 2007.

[3] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[4] G. Matthias, A. Festag, T. Leinmüller, G. Goldacker, and C. Harsch, "Security architecture for vehicular communication," in *WIT 2005*, 2007.

[5] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks (VANET '07)*, pp. 19–28, September 2007.

[6] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Proceedings of the 7th International Conference on Intelligent Transport Systems Telecommunications (ITST '07)*, pp. 339–344, June 2007.

[7] L. Huang, K. Matsuura, H. Yamanet, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '05)*, vol. 2, pp. 1187–1192, March 2005.

[8] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: a practical pseudonym changing scheme for location privacy in VANETs," in *Proceedings of the IEEE Vehicular Networking Conference (VNC '09)*, October 2009.

[9] J. Freudiger, M. Raya, M. Félegyhazi, P. Papadimitratos, and J. -P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proceedings of the 1st International Workshop on Wireless Networking For Intelligent Transportation Systems (Win-ITS '07)*, 2007.

[10] A. M. Carianha, L. P. Barreto, and G. Lima, "Improving location privacy in mix-zones for VANETs," in *Proceedings of the 30th IEEE International Performance, Computing and Communications Conference (IPCCC '11)*, November 2011.

[11] H. Xiong, Z. Chen, and F. Li, "Efficient and multi-level privacy-preserving communication protocol for VANET," *Computers and Electrical Engineering*, vol. 38, no. 3, pp. 573–581, 2012.

[12] B. K. Chaurasia and S. Verma, "Conditional privacy through ring signature in vehicular ad-hoc networks," in *Transactions on Computational Science XIII*, vol. 6750, pp. 147–156, 2011.

[13] D. Boneh, E. -J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Theory of Cryptography*, pp. 325–334, Springer, Berlin, Germany, 2005.

[14] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in CryptologyASIACRYPT*, pp. 552–565, Springer, Berlin, Germany, 2001.

[15] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," in *Public Key CryptographyPKC*, vol. 4450, pp. 166–180, 2007.

[16] J. Groth, R. Ostrovsky, and A. Sahai, "Perfect non-interactive zero knowledge for NP," in *Advances in Cryptology-EUROCRYPT*, vol. 4004, pp. 339–358, Springer, Berlin, Germany, 2006.

[17] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: an effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012.

[18] Y. Pan and L. Jianqing Li, "Cooperative pseudonym change scheme based on the number of neighbors in VANETs," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599–1609, 2013.