An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications

Yipin Sun, *Student Member, IEEE*, Rongxing Lu, *Student Member, IEEE*, Xiaodong Lin, *Member, IEEE*, Xuemin (Sherman) Shen, *Fellow, IEEE*, and Jinshu Su, *Member, IEEE*

***Abstract*—In this paper, we propose an efficient pseudonymous authentication scheme with strong privacy preservation (PASS), for vehicular communications. Unlike traditional pseudonymous authentication schemes, the size of the certificate revocation list (CRL) in PASS is linear with the number of revoked vehicles and unrelated to how many pseudonymous certificates are held by the revoked vehicles. PASS supports the roadside unit (RSU)-aided distributed certificate service that allows the vehicles to update certificates on road, but the service overhead is almost unrelated to the number of updated certificates. Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries cannot trace any vehicle, even though all RSUs have been compromised. Extensive simulations demonstrate that PASS outperforms previously reported schemes in terms of the revocation cost and the certificate updating overhead.**

***Index Terms*—Anonymous authentication, privacy preservation, revocation, vehicular communications.**

I. Introduction

THE VEHICULAR ad hoc network (VANET), as a special kind of mobile ad hoc network, has been subject to extensive research efforts not only from the government but also from academia and the automobile industry in recent years. Different from the traditional ad hoc networks, the VANET contains not only mobile nodes—vehicles—but stationary roadside units (RSUs) as well. Due to this hybrid architecture, the VANET opens new doors to facilitating road safety and traffic management and providing multimedia services for vehicles on the road. According to the dedicated short-range communications (DSRC) [1] in road safety-related applications, each vehicle equipped with onboard units (OBUs) will broadcast routine traffic messages with the information of position, current time, direction, speed, acceleration/deceleration, and traffic events, etc. With this information, drivers can be better aware of their driving environment and take early action to respond to an abnormal situation, such as a traffic accident. However, before putting this attractive application into practice, security and privacy issues in VANETs must be resolved [2]–[5]. Without security and privacy guarantees, an adversary to a VANET can either forge bogus information to mislead other drivers, and even cause a deliberate traffic accident, or track the locations of the interested vehicles by collecting their routine traffic messages. Therefore, how to achieve anonymous authentication has become a fundamental requirement for securing VANETs.

Over the past years, many anonymous authentication schemes have been reported [5]–[13], where both the group-signature-based schemes [6]–[8] and the pseudonymous authentication schemes [5], [9]–[13] can well address most of the security and privacy concerns in VANETs. However, due to the limitations of bandwidth and computation power, the applicability of these reported schemes is questionable in VANETs. The size of the certificate revocation list (CRL) and the checking cost are two important performance metrics for the revocation mechanism in VANETs. Unfortunately, the pseudonymous authentication schemes are prone to generating a huge CRL [5], whereas the checking cost in the group-signature-based schemes is unacceptable for the vehicles with limited computation power. Since the CRL is usually transmitted by vehicle-to-vehicle communication [14], [15], the quick increase of the CRL in the pseudonymous authentication schemes brings large communication cost. Moreover, the larger the CRL size, the longer the transmission delay to all vehicles, and during this period, the misbehaving vehicles can compromise VANETs continually. In the group-signature-based schemes [6]–[8], each checking operation that matches a message signature with respect to an identity in the CRL involves two pairing calculations, which causes obvious computation overhead for a vehicle, e.g., 10^{-2} s in [8]. Given that the CRL usually contains 10 revoked identities and a vehicle receives 20 messages/s, the total checking cost is 2 s.

The distributed certificate service (DCS) is a promising approach to decrease revocation cost [9]–[12]. This way, vehicles can update their pseudonymous certificate sets from the

Manuscript received December 16, 2009; revised March 29, 2010; accepted May 4, 2010. Date of publication June 7, 2010; date of current version September 17, 2010. This work was supported in part by the National Grand Fundamental Research 973 Program of China under Grants 2005CB321801 and 2009CB320503, by the National 863 Development Plan of China under Grants 2008AA01A325 and 2009AA01Z423, by the National Science Foundation of China under Grant 90604006, and by the Natural Sciences and Engineering Research Council of Canada. The review of this paper was coordinated by Dr. J. Deng.

Y. Sun and J. Su are with the School of Computer Science, National University of Defense Technology, Changsha 410073, China (e-mail: ypsun@nudt.edu.cn; sjs@nudt.edu.cn).

R. Lu and X. Shen are with the Centre for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: rxlu@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada (e-mail: xiaodong.lin@uoit.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2010.2051468

TABLE I
RSU DENSITY AND NUMBER OF CERTIFICATES THAT A VEHICLE HAS TO UPDATE ONCE IN NEW YORK CITY [12]

number of required RSUs	size of certificate set
176760	1
1473	120
589	300

certificate issuer by vehicle-to-RSU (V2R) communication on the road. Once each certificate has a short-time period and is used in a specifically geographic region, the CRL that broadcasted in a region can decrease. However, the CRL size still depends on how many pseudonymous certificates are held by the revoked vehicles. Moreover, the certificate updating overhead becomes a heavy burden when the availability of an RSU is not pervasive, particularly in the early stage of RSU deployment [5]. Recently, Wasef *et al.* [12] have studied the relationship between the RSU density in New York City and the number of certificates that a vehicle has to update once, as shown in Table I. From the table, we can see that a vehicle has to update 120 pseudonymous certificates each time if 1473 RSUs had been built. Due to the limited wireless channel bandwidth, it is inefficient and difficult for an RSU to transmit hundreds of certificates for each passing-by vehicle while providing infotainment dissemination services at the same time. Furthermore, to generate so many certificates for tens of thousands of requesters in a short time, the certificate issuer should have very strong computation power, which is a costly expenditure. More seriously, some greedy users may send multiple requests to get more pseudonymous certificates, and legitimate users could also retransmit their request if the service latency becomes large. Subsequently, it will aggravate the service burden and even bring down the certificate issuer. To the best of our knowledge, how to optimize the certificate updating overhead in DCS has not been well addressed in previously reported works.

Another important issue in DCS is the privacy risk when each RSU acts as a subcertificate issuer [9], [11], [12]. To keep a centralized certificate issuer from being a bottleneck, an RSU is allowed to issue certificates for the vehicles. However, it brings a privacy risk when an RSU is compromised by the adversaries. Once the service records of an RSU are leaked, it is easy for the adversary to link the pseudonymous certificates that a vehicle has obtained from the compromised RSU. In particular, when the number of compromised RSUs increases, it possibly provides a solution for the adversaries to revert the mobile trace of the interested vehicles. However, the privacy preservation against the RSUs is still an open issue to any scheme that supports the RSU-aided DCS.

In this paper, to address both security and performance challenges in VANETs, we propose an efficient pseudonymous authentication scheme with strong privacy preservation (PASS) for vehicular communications. PASS supports RSU-aided distribution certificate service that allows a vehicle to update its certificate set from an RSU on the road. The contributions of this paper are fourfold.

1) First, we design a novel scheme to generate the pseudoidentities of the pseudonymous certificates belonging to the same owner based on one-way hash-chain technology. It is easy to revoke the unexpired certificates of a revoked user by only releasing two hash seeds. Therefore, unlike traditional pseudonymous authentication schemes, the CRL size in PASS is only linear with the number of revoked vehicles and unrelated to the number of pseudonymous certificates held by the revoked vehicles.
2) Second, we propose an efficient certificate-updating scheme. Although only the pseudonymous certificates issued by a legitimate RSU are valid in vehicular communication, PASS allows a vehicle to store a large set of pseudonymous certificates issued by the trusted authority (TA). Based on the proxy re-signature cryptography technology [16], where a semitrusted proxy with some information given can turn a user's signature on a message into another user's signature on the same message, the vehicle only needs to request the re-signature keys from an RSU and re-sign numbers of the certificates issued by the TA to be the same as those issued by the RSU itself. This way, the service overhead is almost unrelated to the number of updated certificates.
3) Third, we provide strong privacy preservation to the vehicles. Although the RSUs act as certificate issuers in PASS, they do not know what certificates are held by a vehicle. Therefore, the adversaries cannot trace the interested vehicles although they had compromised all RSUs.
4) Finally, extensive simulations evaluate the proposed scheme and the previously reported schemes on several performance metrics, such as authentication overhead, revocation overhead, and certificate updating overhead on road.

The remainder of this paper is organized as follows: Section II surveys some related works. Section III presents the system model, the threat model, and the research objectives. Section IV gives some preliminaries, including the secure hash function, bilinear pairings, and Schnorr signature algorithm. Then, Section V presents the proposed PASS scheme, followed by the security analysis and performance evaluation in Sections VI and VII, respectively. Finally, Section VIII draws our conclusions.

II. RELATED WORK

Anonymous authentication is a very active topic for securing VANETs and can be roughly divided into two categories, namely, the group-signature-based schemes [6]–[8] and the pseudonymous authentication schemes [5], [9]–[13]. Both of them can address the security requirements well, such as authentication, nonrepudiation, identity revocation, and conditional anonymity. In the group-signature-based schemes, utilizing group signatures [17], any public entity will not reveal the originator identity of a routine traffic message [6], [7]. However, one limitation is that the cost for signing and verifying messages is far more than adopting the traditional public-key-based signature. To reduce these overheads, Calandriello *et al.* [8] propose the Hybrid scheme, wherein a vehicle can issue a certificate for itself by using a group key and then signing its

messages using the public-key-based signature. In such a way, the average overhead of message authentication can decrease. From the viewpoint of revocation cost, the group-signature-based schemes have an advantage that the CRL size is linear with the number of revoked vehicles, but the checking operation involves two pairing calculations, which could take about 10^4 times the computation cost than a string comparison [8].

The pseudonymous authentication schemes [5], [9]–[13] adopt the traditional public-key-based digital signature. Raya and Hubaux [5] propose the basic idea of the pseudonymous authentication scheme (denoted BP in the following context) that each vehicle is supposed to store a large set of pseudonymous certificates with pseudoidentities and randomly chooses one of the available pseudonymous certificates for signing a message at one time. However, when a vehicle is revoked, all the pseudoidentities, e.g., 43 800 identities in [5], would be added into a CRL. Thus, the CRL quickly increases. Two works investigate how to distribute the CRL efficiently by vehicle-to-vehicle communication [14], [15]. However, due to the limited bandwidth of wireless communication and the high-speed mobility of vehicles, it is difficult to distribute a large CRL to all vehicles in a timely fashion. To decrease the CRL size, Bellur [10] suggests segmenting a country into a number of geographic regions and assigning region-specific certificates with a validity period to a vehicle. Lu *et al.* [9] develop the efficient conditional privacy preservation (ECPP) protocol, which is the first protocol to support legitimate vehicles updating short-time pseudonymous certificates from the RSUs frequently. Under the most ideal condition that one RSU is deployed for 600 m along each road, a vehicle takes only one pseudonymous certificate with a quiet short validity period so that it becomes unnecessary for the vehicles to have a copy of CRL. Wasef *et al.* [12] extend RSU-aided distribute certificate service into a hierarchical authority architecture and propose an efficient DCS scheme that supports batch signature verification. Jiang *et al.* [13] propose a batch verification scheme based on binary authentication tree and analyze the message authentication cost when some received messages attach bogus signatures. However, the performance of the aforementioned DCS schemes [9]–[12] largely depends on the RSU density. The fewer the number of RSUs, the larger the revocation cost and the certificate-updating cost.

Another privacy-related study in VANETs focuses on strengthening the location privacy of drivers. Anonymous authentication cannot prevent a vehicle from being traced if the adversary can eavesdrop the whole area. They can link traffic routine messages broadcasted by a same vehicle based on the spatial and temporal correlations between successive locations of the vehicle. Hence, to strengthen the location privacy, some studies [18]–[20] suggest constructing certain regions where the adversary cannot eavesdrop the vehicular communication, called mix zones. Then, vehicles can change certificates when passing through a mix zone. Usually, mix zones should be placed in locations with high node density and unpredictable mobility.

Our proposed PASS is a pseudonymous authentication scheme and supports DCS. Compared with previously reported pseudonymous authentication schemes, it can optimize not only the revocation overhead but the certificate updating overhead as well. More importantly, PASS is the first study on privacy preservation against the subcertificate issuer, i.e., the RSUs in this paper.

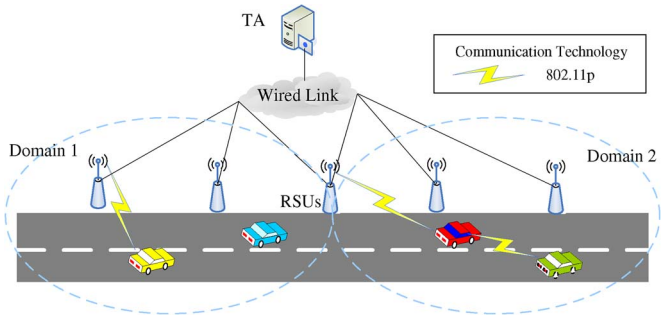


Fig. 1. System model.

III. System Model, Threat Model, and Research Objectives

In this section, we formalize the system model and the threat model and identify the research objectives.

A. System Model

We consider a typical VANET, which consists of a top TA, some stationary RSUs deployed at the roadsides, and a large number of vehicles equipped with OBUs moving on the road, as shown in Fig. 1.

1) The TA is fully trusted by all parties in the system and in charge of the registration of RSUs and vehicles. The TA can divide its huge precinct into several domains and deploy RSUs at the boundary between these domains. The domain information is available to all entities. As usual, the TA is assumed powered with sufficient storage capability and is infeasible for any adversary to compromise [9].
2) RSUs act as the infrastructure of the VANET and connect with the TA by wired links in the system. They provide service for information dissemination and certificate updating. In general, the density of RSU varies in different domains. Without loss of generality, the cantonal domains are supposed to have similar RSU density, whereas the domains in suburb may have a small number of RSUs. The pseudonymous certificates issued by an RSU can only be used in the domain where the RSU is located. As a distributed unit is deployed on the roadside, an RSU has a risk to be compromised. Although the TA can detect a compromised RSU and take action to recover it [9], the records stored in the RSU may have been leaked.
3) Vehicles equipped with OBUs mainly communicate with each other to share local traffic information and improve the driving experience. A vehicle frequently requests the certificate service from an RSU and obtains enough certificates for the following period until passing by another RSU. Obviously, the number of updated pseudonymous certificates depends on the RSU density [12]. The vehicle

periodically changes the pseudonymous certificates to sign routine traffic messages.

B. Threat Model

We name any node to be an adversary or attacker if it deviates from the legitimate VANET protocols or infringes a driver's privacy. In addition, we refer to adversaries as misbehaving nodes in this paper. It is worth noting that an adversary may be an authenticated member of the network. Specifically, in our threat model, we consider that an adversary could diffuse wrong information in the network to affect the behavior of other drivers or harm the infrastructure of VANETs [2], [5]. Moreover, an adversary can also launch tracking attacks by installing receivers on the roads to eavesdrop the messages broadcast by the vehicles. Then, by trying to correlate some of the broadcasted certificates to a vehicle, the adversary may be able to track that vehicle of his interest [12].

C. Research Objectives

Since the VANET is a large-scale wireless network scenario for public service, it faces serious security and privacy challenges. In the PASS scheme, we aim to achieve the following security and privacy objectives.

1) *Authentication:* This includes entity authentication and message integrity. Entity authentication enables receivers to check the authenticity of the sender, whereas message integrity ensures that the content of a message has not been altered in transit. All accepted messages should be from legal members and delivered unaltered.
2) *Nonrepudiation:* No entity can deny the messages generated by itself. It is necessary for accident investigations that the malicious user should pay the fiddler for misleading the victims.
3) *Identity revocation:* It should be possible to exclude an unexpired membership from the VANET. It is a fundamental requirement to defend inside attacks and restore the security of the VANET.
4) *Conditional anonymity:* It means that the TA can reveal the real identity of the members, whereas other entities could neither identify the real identity nor correlate these messages signed by the same member in the long term. In pseudonymous authentication schemes, conditional anonymity is supposed to be held if the validity period length of a pseudonymous certificate is less than a threshold (denoted ΔT), e.g., 1 min [5].
5) *Backward privacy:* Once a membership has been revoked, it should reveal no information that decreases the conditional anonymity for the same member in the period before the revocation takes effect. Moreover, by taking into consideration the limited wireless bandwidth and valuable computation power, we also focus on the following performance objectives.
6) *Authentication overhead:* This mainly includes three parts, namely, message signing cost, verification cost, and communication overhead, which includes the certificate and the signature, as shown in Table II.

TABLE II
FORMAT OF THE SIGNED MESSAGE

protocol version	type	payload	certificate	signature

TABLE III
NOTATIONS

symbol	notation
ΔT	The privacy requirement on the validity period length of a pseudonymous certificate
TS_j	The j-th time slot
TW_k	The k-th time window that consists of L_w time slots
TA	The trust authority
R_x	The x-th RSU
V_i	The i-th vehicle
s	The master secret key of TA
P_{pub}	The master public key of TA
E	An arbitrary entity, which could be a vehicle, an RSU or the TA
$*$	The extra information declaration if it is not empty
$PK_{E,*}$, $SK_{E,*}$	The public key and secret key of E
$\mathsf{Cert}_{E_1,E_2,*}$	A certificate of E_2 issued by E_1
$\sigma_{E,*}$	A signature signed by E
VP_*	The certificate validity period
t_{stamp}	Time stamp
$h(.)$	A hash function such as SHA-1
$f(.)$	A hash function as $\{0,1\}^* \rightarrow \mathbb{G}$
$Enc_\kappa(.)$	A secure symmetric encryption algorithm with secret key κ
$\mathsf{Sign}(SK_E, M)$	Signing the message M by Schnorr signature algorithm with the secret key SK_E
$\mathsf{Verify}(PK_E, M, \sigma_{E,M})$	Verifying the Schnorr signature $\sigma_{E,M}$ of the message M with the public key PK_E
$\|$	Message concatenation operation, which appends several messages together

7) *Revocation overhead:* This can be evaluated by the CRL size and the checking cost against the CRL. Compared with the traditional pseudonymous authentication scheme, we hope to keep the CRL size linear with the number of revoked vehicles. Moreover, PASS is designed to support DCS to decrease the CRL size.
8) *Overhead for certificate updating on the road:* To solve a certificate-updating request, the V2R communication overhead and the computation cost for the certificate issuer (RSU) is expected to be unrelated to the number of updated certificates.

IV. PRELIMINARIES

In this section, we introduce some preliminaries, including secure hash chains, bilinear pairings [21], and the Schnorr signature algorithm [22], which are the bases of our proposed PASS scheme. In addition, the notations used throughout this paper are given in Table III.

A. Hash Chains

A one-way hash function $h(.)$ is said to be secure if the following properties are satisfied [23]: 1) $h(.)$ can take a message of arbitrary length as input and produce a message digest of a fixed-length output; 2) given x, it is easy to compute $h(x) = y$. However, it is hard to compute $h^{-1}(y) = x$ given y; and 3) given x, it is computationally infeasible to find $x' \neq x$ such that $h(x') = h(x)$. Furthermore, supposing that $h^i(x) = h(h^{i-1}(x))$, a hash chain of length L, i.e., $\{S_i\}$, is

constructed by recursively applying $h(.)$ to an initial seed value SD, where $S_i = h^i(\text{SD})$, $i \in [1, L]$. Obviously, given S_i, it is easy to compute $S_j = h^{j-i}(S_i)(j > i)$ but infeasible to obtain S_{i-1}.

B. Bilinear Pairing

Let $\mathbb{G}$ be a cyclic additive group generated by P, and let $\mathbb{G}_T$ be a cyclic multiplicative group of the same prime order q, i.e., $|\mathbb{G}| = |\mathbb{G}_T| = q$. An efficient admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is satisfied with the following properties: 1) *bilinear*: For all $P, Q, R \in \mathbb{G}$, and $a, b \in \mathbb{Z}_q^*$, $e(Q, P + R) = e(P + R, Q) = e(P, Q) \cdot e(R, Q)$. In particular, $e(aP, bQ) = e(P, Q)^{ab}$; 2) *nondegenerate*: There exist $P, Q \in \mathbb{G}$ such that $e(P, Q) \neq 1_{\mathbb{G}_T}$; and 3) *computable*: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in \mathbb{G}$. Such an admissible bilinear map e can be constructed by the modified Weil or Tate pairings on the elliptic curves [21]. The group that possesses such a map e is called a bilinear group, from which two problems are believed hard.

1) *Elliptic curve discrete logarithm problem (ECDLP)*: Given a point P of order q on an elliptic curve and a point Q on the same curve, the ECDLP problem [21] is to determine the integer $l, 0 \leq l \leq q - 1$, such that $Q = lP$.
2) *Computational Diffie–Hellman problem (CDH):* Given two unknowns $a, b \in \mathbb{Z}_q^*$, the CDH problem [21] is given $P, aP, bP \in \mathbb{G}$; compute $abP \in \mathbb{G}$.

C. Schnorr Signature Algorithm

The Schnorr signature algorithm [22] will be adopted as the basis of the signatures signed by the TA and vehicles, which is efficient and provably secure in the random oracle model. Suppose an entity E has the private secret key SK_E and the public key PK_E, where $\text{SK}_E \in \mathbb{Z}_q^*$, and $\text{PK}_E = \text{SK}_E \cdot P$. Let $\mathsf{Sign}(\text{SK}_E, M)$ denote the procedure that the entity E signs a signature $\sigma_{E,M}$ on message M, and let $\mathsf{Verify}(\text{PK}_E, M, \sigma_{E,M})$ denote the procedure that other entities verify the Schnorr signature $\sigma_{E,M}$ of M signed by the entity E.

V. Our Proposed PASS Scheme

In this section, we will present our PASS scheme, which mainly consists of six phases: 1) system initialization; 2) RSU certificate issuing; 3) vehicle pseudonymous certificate issuing; 4) vehicle pseudonymous certificate updating; 5) identity revocation; and 6) message signature and verification.

A. System Initialization

Given the bilinear parameters $(q, \mathbb{G}, \mathbb{G}_T, e, P)$, the TA initializes the system by running the following steps.

1) The TA chooses one random number $s \in \mathbb{Z}_q^*$ as the master secret key and computes the master public key $P_{\text{pub}} = sP \in \mathbb{G}$.
2) The TA chooses two one-way hash functions $h(.)$, e.g., SHA-1, and $f(.) : \{0, 1\}^* \to \mathbb{G}$ and a secure symmetric encryption algorithm $\text{Enc}_\kappa(.)$.
3) The TA chooses ΔT according to the privacy requirements of most vehicles and sets the validity period of the pseudonymous certificate equal to ΔT. Then, the TA estimates the number of certificates that a vehicle has to update from an RSU once according to the RSU density in each domain [12] and selects a cut-point that satisfies the requirement of most cantonal domains, which is denoted L_w. Furthermore, the updated certificates in a domain D_y will be counted by L_w, i.e., $N_y * L_w$, where $N_y \in \mathbb{N}$. In a suburb domain D_y that has fewer RSUs, $N_y > 1$. After that, the time domain is divided into serial time slots by ΔT and serial time windows by $L_w * \Delta T$; thus, a time window includes L_w time slots. This way, a pseudonymous certificate can only be used in one time slot. Let TS_j denote the jth time slot that ends at $j * \Delta T$, and let TW_k denote the kth time window that ends at $k * L_w * \Delta T$. TS_j is in TW_k if $j \in ((k-1) * L_w, k * L_w]$. Then, the system parameters will be published, which include $(q, \mathbb{G}, \mathbb{G}_T, e, P, P_{\text{pub}}, h(.), f(.), \text{Enc}_\kappa(.), \Delta T, L_w)$.

B. RSU Certificate Issuing

For an RSU R_x in the domain D_y, the TA issues a certificate $\mathsf{Cert}_{\text{TA},R_x}$, as shown in the list that follows.

1) The TA chooses a random number $r \in \mathbb{Z}_q^*$ and sets the secret key $\text{SK}_{R_x} = r$ and the public key $\text{PK}_{R_x} = rP$.
2) The TA generates the signature σ_{TA,R_x} using the Schnorr signature algorithm, where $\sigma_{\text{TA},R_x} = \mathsf{Sign}(s, \text{PK}_{R_x} \| D_y)$.
3) The TA securely delivers SK_{R_x} and $\mathsf{Cert}_{\text{TA},R_x}$ to R_x, where $\mathsf{Cert}_{\text{TA},R_x} = (\text{PK}_{R_x}, D_y, \sigma_{\text{TA},R_x})$. Then, it stores the mapping between the real ID of R_x and $\mathsf{Cert}_{\text{TA},R_x}$.

R_x and the other entities can verify the certificate $\mathsf{Cert}_{\text{TA},R_x}$ by the procedure $\mathsf{Verify}(P_{\text{pub}}, \text{PK}_{R_x} \| D_y, \sigma_{\text{TA},R_x})$.

C. Vehicle Pseudonymous Certificate Issued by the TA

PASS adopts a prestore strategy, wherein each vehicle can obtain a large set of pseudonymous certificates from the TA during the vehicle inspection. Suppose the TA issues $L_w * C$ pseudonymous certificates corresponding to the period from the time window TW_1 to TW_C for the vehicle V_i. Let $\mathsf{Cert}_{\text{TA},V_i,j}$ denote V_i's pseudonymous certificate in the time slot TS_j $(j \in [1, L_w * C])$, where its validity period $\text{VP}_{V_i,j} = j$. As shown in Fig. 2, the pseudoidentity of $\mathsf{Cert}_{\text{TA},V_i,j}$ is calculated based on two hash chains with the random hash seeds SD_3 and SD_4, i.e., $\text{PID}_{V_i,j} = h(S_{3,j} \oplus S_{4,C*L_w-j+1})$, where $S_{3,j} = h^j(\text{SD}_3)$, $S_{4,C*L_w-j+1} = h^{C*L_w-j+1}(\text{SD}_4)$, and $\oplus$ is XOR operation. This way, all pseudonymous certificates of V_i can easily be revoked by releasing two hash seeds, the details of which will be presented in Section V-E. However, without knowing the two seeds, it is infeasible to reveal the linkability among these certificates.

Different with issuing the certificate for an RSU, the TA does not use its master secret key to sign the pseudonymous certificates for a vehicle directly, but it chooses a temporary secret key for such purpose in each time window. Let $\text{SK}_{\text{TA},V_i,k}$ denote the signing secret key of the TA for issuing V_i's

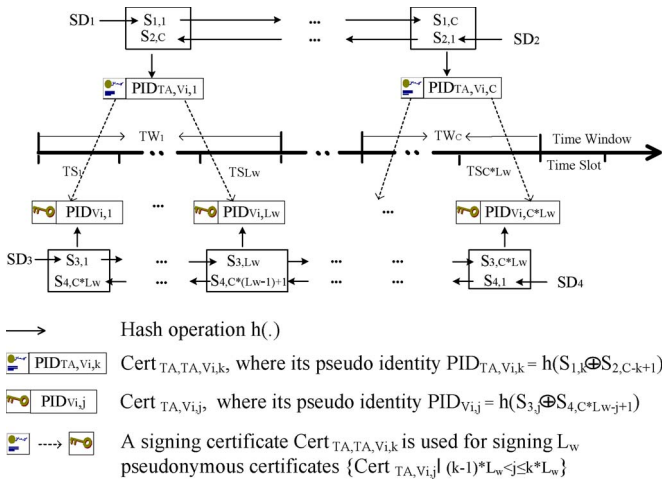


Fig. 2. Signing certificate $\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k}$ and pseudonymous certificate $\mathsf{Cert}_{\mathrm{TA},V_i,j}$.

pseudonymous certificates in the time window TW_k, $\mathrm{PK}_{\mathrm{TA},V_i,k}$ denote the corresponding public key, and $\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k}$ denote the corresponding certificate, named the signing certificate. As shown in Fig. 2, a signing certificate $\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k}$ is used for issuing L_w pseudonymous certificates $\{\mathsf{Cert}_{\mathrm{TA},V_i,j} | j \in ((k-1)*L_w, k*L_w]\}$. In addition, the pseudoidentity of $\mathsf{Cert}_{\mathrm{TA},V_i,j}$ can also be calculated from two hash chains with the random hash seeds SD_1 and SD_2, i.e., $\mathrm{PID}_{\mathrm{TA},V_i,k} = h(S_{1,k} \oplus S_{2,C-k+1})$, where $S_{1,k} = h^k(\mathrm{SD}_1)$, and $S_{2,C-k+1} = h^{C-k+1}(\mathrm{SD}_2)$.

The certificate-issuing procedure is presented in Algorithm 1. First, the TA generates the signing secret keys $\{\mathrm{SK}_{\mathrm{TA},V_i,k}\}$ and the corresponding signing certificates $\{\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k}\}$ for itself based on the Schnorr signature algorithm in lines 2–16, where $k \in [1, C]$. Second, the TA uses each secret key $\mathrm{SK}_{\mathrm{TA},V_i,k}$ to sign L_w pseudonymous certificates based on the short signature algorithm [24] in lines 17–33. After that, the TA sends the secret key set $\{\mathrm{SK}_{V_i,j}\}$, the pseudonymous certificate set $\{\mathsf{Cert}_{\mathrm{TA},V_i,j}\}$, and the signing certificate set $\{\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k}\}$ securely to vehicle V_i. Finally, the TA stores the mapping relationship between the real identity of V_i and all these pseudoidentities and a 7-tuple $\langle V_i, 0, C, \mathrm{SD}_1, \mathrm{SD}_2, \mathrm{SD}_3, \mathrm{SD}_4 \rangle$.

Algorithm 1: Certificate_issue (s, C)

Data: The master secret key s of TA, the time window span C

Result: The secret key and pseudonymous certificate set for vehicle V_i, and the signing certificate set of TA

1 **begin**
2 Select two random seed values SD_1 and SD_2
3 /⋆ generates two hash chains $\{S_{1,k}\}$ and $\{S_{2,k}\}$ ⋆ /
4 **for** *each* $k \in [1, C]$ **do**
5 Set $S_{1,k} = h^k(\mathrm{SD}_1)$, and $S_{2,k} = h^k(\mathrm{SD}_2)$
6 **end**
7 /⋆ issues the signing certificates of TA ⋆/
8 **for** *each* $k \in [1, C]$ **do**
9 Set $\mathrm{PID}_{\mathrm{TA},V_i,k} = h(S_{1,k} \oplus S_{2,C-k+1})$
10 /⋆ generates the signing secret key and public key used in TW_k ⋆ /
11 Select a random number $r_1 \in \mathbb{Z}_q^*$
12 Set $\mathrm{SK}_{\mathrm{TA},V_i,k} = r_1$,
13 $\mathrm{PK}_{\mathrm{TA},V_i,k} = r_1 P$, and $\mathrm{VP}_{\mathrm{TA},V_i,k} = k$
14 Calculate $\sigma_{\mathrm{TA},\mathrm{TA},V_i,k} = \mathbf{Sign}(s, \mathrm{PK}_{\mathrm{TA},V_i,k} \| \mathrm{VP}_{\mathrm{TA},V_i,k} \| \mathrm{PID}_{\mathrm{TA},V_i,k})$
15 Set $\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k} = (\mathrm{PK}_{\mathrm{TA},V_i,k}, \mathrm{VP}_{\mathrm{TA},V_i,k}, \mathrm{PID}_{\mathrm{TA},V_i,k}, \sigma_{\mathrm{TA},\mathrm{TA},V_i,k})$
16 **end**
17 Select two random seed values SD_3 and SD_4
18 /⋆ generates two hash chains $\{S_{3,j}\}$ and $\{S_{4,j}\}$ ⋆ /
19 **for** each $j \in [1, L_w * C]$ **do**
20 Set $S_{3,j} = h^j(\mathrm{SD}_3)$, and $S_{4,j} = h^j(\mathrm{SD}_4)$
21 **end**
22 /⋆ issues the pseudonymous certificates of V_i ⋆ /
23 **for** each $j \in [1, L_w * C]$ **do**
24 Set $\mathrm{PID}_{V_i,j} = h(S_{3,j} \oplus S_{4,C*L_w-j+1})$
25 /⋆ generates the secret key and public key of V_i used in TS_j ⋆ /
26 Select a random number $r_2 \in \mathbb{Z}_q^*$
27 Set $\mathrm{SK}_{V_i,j} = r_2$,
28 $\mathrm{PK}_{V_i,j} = r_2 P$, and $\mathrm{VP}_{V_i,j} = j$
29 /⋆ signs with the signing secret key in TW_k that concludes TS_j ⋆ /
30 Calculate $k = \lceil j / L_w \rceil$, and
31 $\sigma_{\mathrm{TA},V_i,j} = \mathrm{SK}_{\mathrm{TA},V_i,k} \cdot f(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j})$
32 Set $\mathsf{Cert}_{\mathrm{TA},V_i,j} = (\mathrm{PK}_{V_i,j}, \mathrm{VP}_{V_i,j}, \mathrm{PID}_{V_i,j}, \sigma_{\mathrm{TA},V_i,j})$
33 **end**
34 **return** $\{\mathrm{SK}_{V_i,j}, \mathsf{Cert}_{\mathrm{TA},V_i,j}, \mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k} | j \in [1, L_w * C], k \in [1, C]\}$
35 **end**

V_i and other entities can verify the signing certificate $\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k}$ by the procedure $\mathsf{Verify}(P_{\mathrm{pub}}, \mathrm{PK}_{\mathrm{TA},V_i,k} \| \mathrm{VP}_{\mathrm{TA},V_i,k} \| \mathrm{PID}_{\mathrm{TA},V_i,k}, \sigma_{\mathrm{TA},\mathrm{TA},V_i,k})$. Moreover, V_i can verify the pseudonymous certificate $\mathsf{Cert}_{\mathrm{TA},V_i,j}$ by $e(\sigma_{\mathrm{TA},V_i,j}, P) \stackrel{?}{=} e(f(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}), \mathrm{PK}_{\mathrm{TA},V_i,k})$, where $j \in ((k-1) * L_w, k * L_w]$. The verification holds since

$$\begin{aligned} & e(\sigma_{\mathrm{TA},V_i,j}, P) \\ &= e\left(\mathrm{SK}_{\mathrm{TA},V_i,k} \cdot f\left(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}\right), P\right) \\ &= e\left(f\left(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}\right), \mathrm{SK}_{\mathrm{TA},V_i,k} \cdot P\right) \\ &= e\left(f\left(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}\right), \mathrm{PK}_{\mathrm{TA},V_i,k}\right). \end{aligned}$$

Remarks:

1) The TA can carry out Algorithm 1 in advance and then securely deliver these credentials to V_i during the vehicle inspection. This way, certificate issuing is not a real-time procedure. Therefore, the TA cannot become the bottleneck for the system.
2) In PASS, a vehicle takes a large number of pseudonymous certificates, but each pseudonymous certificate validates in different time slots. It can restrict the credential misuse.

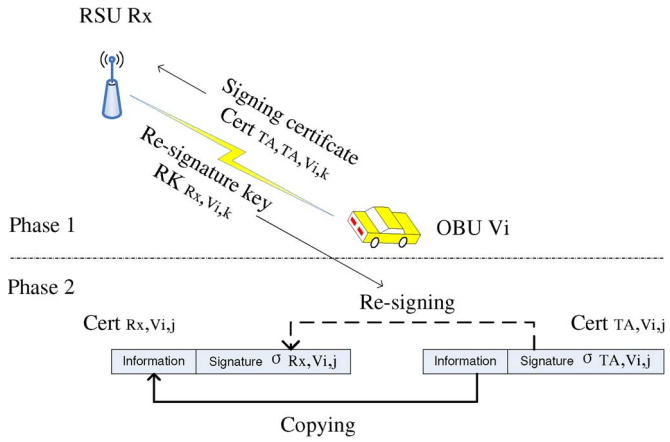


Fig. 3. Pseudonymous certificate updating.

For example, without the strict validity period, a misbehaving vehicle may use all pseudonymous certificates in parallel to impersonate a number of vehicles and mount a Sybil attack [2]. A limitation of the proposed strategy is that a vehicle has to take more certificates than it needs upon driving. However, the storage overhead for a vehicle evaluated in Section VII-D is accessible under the current storage capacity.

D. Vehicle Pseudonymous Certificate Updating

Although a vehicle has a large set of pseudonymous certificates issued by the TA, it cannot use these certificates directly in vehicular communication. In the domain D_y, only the certificates issued by an RSU R_x belonging to this domain are valid. However, a vehicle V_i does not request $N_y * L_w$ certificates from R_x directly. Instead, adopting the proxy re-signature cryptography technology [16], it only needs to request N_y re-signature key from R_x and then re-signs the pseudonymous certificates issued by the TA to be the same as those issued by R_x itself. As shown in Fig. 3, the whole process can be divided into two phases.

Phase 1 (Requesting re-signature key): Given that the current time window is TW_k, V_i can submit the signing certificates $\mathrm{SC} \subseteq \{\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k'} | k' \in [k+1, k+N_y]\}$ to request the corresponding re-signature keys from the R_x.

1) R_x broadcasts its certificate $\mathsf{Cert}_{\mathrm{TA},R_x}$ periodically, e.g., every 5 s.
2) If $\mathsf{Cert}_{\mathrm{TA},R_x}$ is valid, V_i selects a random number $r_3 \in \mathbb{Z}_q^*$ and calculates the shared secret key $\phi = r_3 \cdot \mathrm{PK}_{R_x}$ and the hint $\psi = r_3 P$. Then, it sends the request message $(\psi, \mathrm{Enc}_\phi(t_{\mathrm{stamp}} \| \mathrm{SC})$ to R_x, and t_{stamp} is the time stamp.
3) R_x calculates the shared secret key $\phi' = \mathrm{SK}_{R_x} \cdot \psi$ to decrypt the request message and checks whether t_{stamp} is fresh, and the signing certificates SC are valid during the period from TW_{k+1} to TW_{k+N_y}. If the verification is true, R_x calculates the re-signature key $\mathrm{RK}_{R_x,V_i,k'} = (1/\mathrm{SK}_{R_x}) \cdot \mathrm{PK}_{\mathrm{TA},V_i,k'}$ for each $\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k'} \in \mathrm{SC}$. After that, R_x sends $\{\mathrm{RK}_{R_x,V_i,k'}\}$ back to V_i. Finally, R_x stores the service records that consist of the serial number of the time window and the pseudoidentity of the signing certificate, i.e., $\langle k', \mathrm{PID}_{\mathrm{TA},V_i,k'} \rangle$.
4) V_i verifies each re-signature key in $\{\mathrm{RK}_{R_x,V_i,k'}\}$ by checking that

$$e(\mathrm{RK}_{R_x,V_i,k'}, \mathrm{PK}_{R_x}) \stackrel{?}{=} e\left(\frac{1}{\mathrm{SK}_{R_x}} \cdot \mathrm{PK}_{\mathrm{TA},V_i,k'}, \mathrm{SK}_{R_x} \cdot P\right) = e(\mathrm{PK}_{\mathrm{TA},V_i,k'}, P).$$

Phase 2 (Re-signing pseudonymous certificates): The re-signature key $\mathrm{RK}_{R_x,V_i,k'}$ can be used to re-sign L_w pseudonymous certificates signed by $\mathsf{Cert}_{\mathrm{TA},\mathrm{TA},V_i,k'}$ primitively, i.e., $\{\mathsf{Cert}_{\mathrm{TA},V_i,j} | j \in ((k'-1) * L_w, k' * L_w]\}$. $V_i$transforms $\mathsf{Cert}_{\mathrm{TA},V_i,j} = (\mathrm{PK}_{V_i,j}, \mathrm{VP}_{V_i,j}, \mathrm{PID}_{V_i,j}, \sigma_{\mathrm{TA},V_i,j})$ to the corresponding certificate $\mathsf{Cert}_{R_x,V_i,j}$ issued by R_x here.

5) To re-sign $\sigma_{\mathrm{TA},V_i,j}$ to the signature $\sigma_{R_x,V_i,j} = \{\beta_0, \beta_1, \beta_2\}$ signed by R_x, V_i chooses a random number $r_4 \in \mathbb{Z}_q^*$ and calculates

$$\begin{cases} \beta_0 = r_4 \cdot \sigma_{\mathrm{TA},V_i,j} \\ \beta_1 = r_4 \cdot \mathrm{PK}_{\mathrm{TA},V_i,k'} \\ \beta_2 = r_4 \cdot \mathrm{RK}_{R_x,V_i,k'}. \end{cases}$$

6) V_i composes $\mathsf{Cert}_{R_x,V_i,j} = (\mathrm{PK}_{V_i,j}, \mathrm{VP}_{V_i,j}, \mathrm{PID}_{V_i,j}, \sigma_{R_x,V_i,j}, \mathsf{Cert}_{\mathrm{TA},R_x})$.

To verify $\mathsf{Cert}_{R_x,V_i,j}$, other entities can first check that $\mathsf{Cert}_{\mathrm{TA},R_x}$ is valid and then accept it if $e(\beta_0 + \beta_1, P) \stackrel{?}{=} e(\beta_1, f(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}))e(\mathrm{PK}_{R_x}, \beta_2)$. The verification holds since

$$\begin{aligned}
e(\beta_0, P) &= e(r_4 \cdot \sigma_{\mathrm{TA},V_i,j}, P) \\
&= e\left(r_4 \cdot \mathrm{SK}_{\mathrm{TA},V_i,k'} \cdot f\left(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}\right), P\right) \\
&= e\left(f\left(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}\right), r_4 \cdot \mathrm{SK}_{\mathrm{TA},V_i,k'} \cdot P\right) \\
&= e\left(f\left(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}\right), r_4 \cdot \mathrm{PK}_{\mathrm{TA},V_i,k'}\right) \\
&= e\left(\beta_1, f\left(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}\right)\right) \\
e(\beta_1, P) &= e\left(r_4 \cdot \mathrm{PK}_{\mathrm{TA},V_i,k'}, P\right) \\
&= e\left(r_4 \cdot \frac{\mathrm{SK}_{\mathrm{TA},V_i,k'}}{\mathrm{SK}_{R_x}} \cdot \mathrm{SK}_{R_x} \cdot P, P\right) \\
&= e\left(\mathrm{SK}_{R_x} \cdot P, r_4 \cdot \frac{\mathrm{SK}_{\mathrm{TA},V_i,k'}}{\mathrm{SK}_{R_x}} \cdot P\right) \\
&= e(\mathrm{PK}_{R_x}, r_4 \cdot \mathrm{RK}_{R_x,V_i,k'}) \\
&= e(\mathrm{PK}_{R_x}, \beta_2) \\
e(\beta_0 + \beta_1, P) &= e(\beta_0, P)e(\beta_1, P) \\
&= e\left(\beta_1, f\left(\mathrm{PK}_{V_i,j} \| \mathrm{VP}_{V_i,j} \| \mathrm{PID}_{V_i,j}\right)\right) \\
&\quad \times e(\mathrm{PK}_{R_x}, \beta_2).
\end{aligned}$$

Remarks:

1) The vehicle V_i can obtain at most N_y re-signature keys from R_x once. The greedy users cannot benefit more although they retransmit the request many times. Compared with issuing $N_y * L_w$ certificates, the service burden for R_x is trivial. Although N_y is larger than 1 in a suburb domain, the service cost is acceptable for an RSU because the traffic is small in suburb as well.
2) It is worth noting that a misbehaving vehicle may try to create a pseudonymous certificate with an invalid pseudoidentity to avoid being traced by the TA. However, due to the adopted re-signature cryptography technology, the vehicle cannot generate a correct signature for the forged pseudonymous certificate.
3) R_x can issue pseudonymous certificates for the vehicles by itself. If the TA finds out a valid certificate issued by R_x without the corresponding record in its own database, it means that R_x has been compromised.

E. Identity Revocation

In PASS, the TA publishes the CRLs to revoke the unexpired memberships in every domain. Let $\text{CRL}_{D(y),R}$ denote the CRL for the compromised RSUs in the domain D_y, and let $\text{CRL}_{D(y),V}$ denote the CRL for the revoked vehicles in D_y. $\text{CRL}_{D(y),R}$ and $\text{CRL}_{D(y),V}$ would be broadcast in D_y by vehicle-to-vehicle communication.

To revoke an RSU in D_y, the TA adds its certificate to $\text{CRL}_{D(y),R}$. This way, all the pseudonymous certificate issued by the compromised RSUs would be revoked at the same time.

To revoke a vehicle V_i, the signing certificates stored in V_i should be informed to all RSUs, and the unexpired pseudonymous certificates that V_i had obtained by the re-signing service should be revoked at the same time. In PASS, instead of revoking V_i thoroughly, the TA can just prevent it from accessing VANETs for a certain revocation period, e.g., from the current time window TW_n to the future time window $\text{TW}_m (m \in (n, C])$. The procedure runs here.

1) The TA finds out the 7-tuple $\langle V_i, 0, C, \text{SD}_1, \text{SD}_2, \text{SD}_3, \text{SD}_4 \rangle$ and calculates $S_{1,n} = h^n(\text{SD}_1)$, $S_{2,C-m+1} = h^{C-m+1}(\text{SD}_2)$. Then, it sends the pseudoidentity information of the revoked signing certificates $\langle n, m, S_{1,n}, S_{2,C-m+1} \rangle$ to all RSUs.
2) After receiving $\langle n, m, S_{1,n}, S_{2,C-m+1} \rangle$, an RSU R_x calculates these pseudoidentities $\text{PID}_k (k \in [n, m])$ of revoked signing certificates, where

$$\begin{cases} S_{1,k} = h^{k-n}(S_{1,n}) \\ S_{2,C-k+1} = h^{m-k}(S_{2,C-m+1}) \\ \text{PID}_k = h(S_{1,k} \oplus S_{2,C-k+1}). \end{cases}$$

R_x adds PID_k into the CRL used in the time window TW_k and will not provide the re-signature key for the signing certificate with the pseudoidentity PID_k. R_x also checks whether it had issued the re-signature key for the revoked signing certificate with the pseudoidentity $\text{PID}_{k'}$. If the record does not exist, set $k' = 0$. R_x sends k' back to the TA.
3) After receiving the responses from all RSUs in D_y, the TA finds out the maximum value of $\{k'\}$, which is denoted k''. If the revoked vehicle V_i has the unexpired pseudonymous certificate in D_y, i.e., $k'' \neq 0$, the TA calculates $S_{3,(n-1)*L_w+1} = h^{(n-1)*L_w+1}(\text{SD}_3)$ and $S_{4,(C-k'')*L_w+1} = h^{(C-k'')*L_w+1}(\text{SD}_4)$. Then, it adds the pseudoidentity information of the revoked pseudonymous certificates $\langle (n-1) * L_w, k'' * L_w, S_{3,(n-1)*L_w+1}, S_{4,(C-k'')*L_w+1} \rangle$ to $\text{CRL}_{D(y),V}$. After that, $\text{CRL}_{D(y),V}$ will be distributed to all vehicles in the domain D_y by vehicle-to-vehicle communication [14].
4) After receiving the updated information $\langle (n-1) * L_w, k'' * L_w, S_{3,(n-1)*L_w+1}, S_{4,(C-k'')*L_w+1} \rangle$ in $\text{CRL}_{D(y),V}$, any vehicle can calculate the pseudoidentities $\text{PID}_j (j \in ((n-1) * L_w, k'' * L_w])$ of the revoked pseudonymous certificates, where

$$\begin{cases} S_{3,j} = h^{j-(n-1)*L_w-1}\left(S_{3,(n-1)*L_w+1}\right) \\ S_{4,C*L_w-j+1} = h^{k''*L_w-j}\left(S_{4,(C-k'')*L_w+1}\right) \\ \text{PID}_j = h(S_{3,j} \oplus S_{4,C*L_w-j+1}). \end{cases}$$

Moreover, the vehicle would add PID_j to the local CRL used in the time slot TS_j.

Remarks:

1) No matter how many pseudonymous certificates a revoked vehicle has, only one item needs to be added into the CRL. Therefore, the CRL size is linear in terms of the number of revoked vehicles.
2) Although the local CRL for each vehicle varies in different time slots, the constructing overhead can be omitted because the vehicle can construct CRL_j using the idle computation time in the time slot TS_{j-1}.

F. Message Signature and Verification

In the time slot TS_j, a vehicle V_i should use the pseudonymous certificate $\mathsf{Cert}_{R_x,V_i,j}$ to sign a message M by the Schnorr signature algorithm, i.e., the signature $\sigma_{V_i,M} = \mathsf{Sign}(\text{SK}_{V_i,j}, M)$.

After receiving the message $(M, \sigma_{V_i,M}, \mathsf{Cert}_{R_x,V_i,j})$ from V_i, the other entities first verify whether $\mathsf{Cert}_{R_x,V_i,j}$ is valid and then accept the message if $\mathsf{Verify}(\text{PK}_{V_i,j}, M, \sigma_{V_i,M})$ is true.

Remarks: According to DSRC, a vehicle broadcasts a routine traffic message every 300 ms. Because the validity period of a pseudonymous certificate is usually 1 min [8], it means that each certificate is used to sign about 200 messages. It is efficient for any vehicle to keep a public key buffer for the verified pseudonymous certificates so that the pseudonymous certificates of the neighboring vehicles only need to be verified once. Moreover, a vehicle can broadcast its pseudonymous certificate periodically, e.g., 1 s, whereas it attaches the public key with every message instead of the whole certificate. It is good for reducing communication cost.

VI. Security Analysis

In this section, we discuss security issues of the proposed PASS scheme according to the security objectives presented in Section III-C.

A. Authentication and Nonrepudiation

During routine vehicular communication, authentication and nonrepudiation are achieved by the public-key-based digital signatures. First, the secret key of any entity in PASS is secure. It can be seen that finding the master secret key s from the master public key $P_{\rm pub} = sP$ is an instance of the ECDLP problem. A similar analogy applies to finding the secret key SK_E of any entity E from the corresponding public key PK_E, where $\mathrm{PK}_E = \mathrm{SK}_E \cdot P$. Second, based on the well-known signature algorithms such as the Schnorr signature, the short signature, and the re-signature technology, the signature generated by each entity is unforgeable. Therefore, entity authentication can be achieved by a digital certificate that consists of the owner's public key and the issuer's signature. Similarly, the message with a veritable signature can guarantee message integrity and nonrepudiation.

In addition, weak authentication for certificate updating is secure. As presented in Section V-D, the vehicle V_i uses a signing certificate of the TA as the credential to get service from R_x. Although this authentication process is not as strong as the request message is supposed to attach V_i's signature, it achieves the tradeoff between efficiency and security. First, except for the TA and V_i, the signing certificate is only explored to R_x because the communication between V_i and R_x is confidential. Finding the shared secret key ϕ from ψ and PK_{R_x} is an instance of the CDH problem: given P, $\psi = r_3 P$, and $\mathrm{PK}_{R_x} = \mathrm{SK}_{R_x} \cdot P$, find $\phi = r_3 \cdot \mathrm{SK}_{R_x} \cdot P$. If R_x is compromised but not detected by the TA, the adversaries may utilize the received signing certificates to launch denial-of-service (DoS) attack against the other legitimate RSUs. However, with the help of the vehicles who own these signing certificates, the TA can easily discover the compromised RSU and revoke it. Second, the re-signature key generated for a signing certificate can only be used to re-sign these pseudonymous certificates that are signed by the signing certificate. It is useless for the other entities except V_i. Therefore, the re-signature key can be transmitted as a clear text. Finally, the time stamp that is attached in the request messages can prevent the replay attack to an RSU.

B. Identity Revocation

In PASS, the TA can exclude an entity from the VANET by revoking its unexpired certificates with a CRL. Specially, to prevent a vehicle from accessing the VANET, the TA releases only two hash elements corresponding to the revocation period. Then, other entities can compute the pseudoidentities of the pseudonymous certificates held by the revoked vehicle and drop the messages signed by these certificates.

C. Conditional Anonymity

In PASS, conditional anonymity is preserved by the following techniques.

1) *Pseudonymous authentication:* A vehicle frequently changes pseudonymous certificates during vehicular communication. Moreover, other entities except the TA cannot reveal the relationship between these certificates without knowing these two hash seeds. For example, given two pseudoidentities $\mathrm{PID}_{V,1} = h(S_{3,1} \oplus S_{4,C*L_w})$ and $\mathrm{PID}_{\overline{V},2} = h(\overline{S}_{3,2} \oplus \overline{S}_{4,C*L_w-1})$, to verify their relationship, the adversary first computes $x = h^{-1}(\mathrm{PID}_{V,1})$ and then computes $y = h^{-1}(x \oplus S_{3,1})$ for each possible value of $S_{3,1}$ until the verification is true, i.e., $h(h(S_{3,1}) \oplus y) \stackrel{?}{=} \mathrm{PID}_{\overline{V},2}$. For an l-bit one-way hash function, the expected cost of solving h^{-1} is $O(2^{l-1})$. Moreover, suppose $\mathrm{PID}_{V,1}$ and $\mathrm{PID}_{\overline{V},2}$ really belong to the same user, the expected number of h^{-1} operation to confirm this relationship is 2^{l-1}. Therefore, the total cost is $O(2^{2l-2})$. Given a 160-bit one-way hash function such as SHA-1, it is a hard computational problem to verify the relationship between two pseudoidentities. In addition, to prevent a vehicle from being traced, it is better for the vehicle to change certificates in a mix zone [18]–[20].
2) *Anonymous authentication for certificate updating:* A vehicle requests service from the RSUs by the different signing certificates of the TA. Similar to the aforementioned analysis, without knowing two hash seeds, RSUs cannot find out the relationship between these pseudoidentities of the signing certificates submitted by the interested vehicle.
3) *Certificate updating based on re-signature technology:* Although an RSU R_x acts as the certificate issuer for a vehicle V_i, it has no idea about infringing on V_i's privacy. First, R_x does not know the pseudoidentity of the pseudonymous certificates held by V_i because the re-signing operation is implemented by V_i itself. Second, although the new certificate signature $\sigma_{R_x,V_i,j}$ is generated with the re-signature key $\mathrm{RK}_{R_x,V_i,k'}$ issued by R_x, it is impossible to tell the relationship between the signature $\sigma_{R_x,V_i,j}$ and $\mathrm{RK}_{R_x,V_i,k'}$ without knowing the random number r_4.

D. Backward Privacy

In PASS, after a vehicle is revoked, it is still difficult for any entity to reduce the pseudoidentities of pseudonymous certificates used by the revoked vehicle in the past. For example, suppose $S_{3,j}$ and $S_{4,1}$ are released to revoke a vehicle V_i from the time slot TS_j. To compute V_i's pseudoidentity in the time slot TS_{j-1}, i.e., $\mathrm{PID}_{V_i,j-1} = h(S_{3,j-1} \oplus S_{4,C*L_w-j+2})$, the adversary has to know $S_{3,j-1} = h^{-1}(S_{3,j})$ at first. Given a 160-bit one-way hash function such as SHA-1, it is hard to find out $S_{3,j-1}$ from $S_{3,j}$.

Among the previously reported works, the group-signature-based schemes cannot achieve backward privacy, whereas the pseudonymous authentication schemes can achieve the aforementioned objectives basically if they use short-time pseudonymous certificates. However, the schemes that adopt RSU-aided DCS cannot achieve conditional anonymity against the RSUs. For example, in ECPP, a vehicle requests pseudonymous

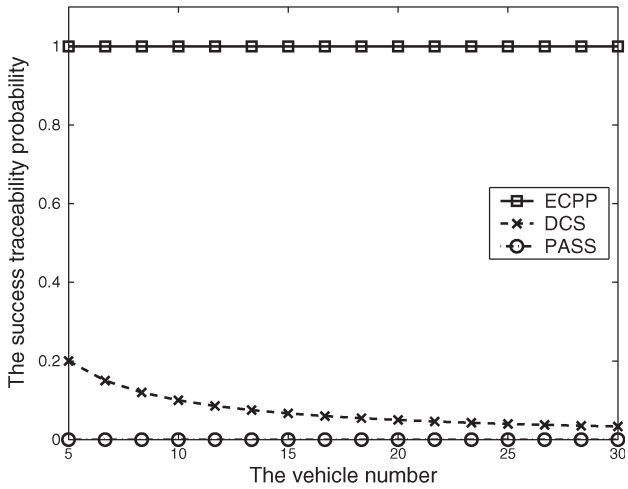


Fig. 4. Success traceability probability when the RSU is compromised.

certificates from an RSU by its invariable credential. Therefore, when the service records stored in an RSU are leaked, the adversary can find out all the certificates that the RSU has issued for the interested vehicle. In DCS, a vehicle obtains the RSU service by a pseudonymous certificate issued by the other RSUs. This way, the adversary does not know which vehicle requests the service, but it can correlate the pseudonymous certificates belonging to the same user. Here, we develop a probabilistic model to analyze the risk that the knowledge of an RSU is used to track an interested vehicle.

Suppose there is an RSU, an adversary, and λ vehicles in a certain region. The adversary gathers some traffic routine messages during ξ time slots and tries to analyze the mobile route of an interested vehicle. In each time slot, the adversary has recorded the certificates used by these vehicles. Let $\Pr(\theta)$ denote the probability that the adversary distinguishes the pseudonymous certificate of the interested vehicle from θ candidate certificates, where $\Pr(\theta) = 1/\theta$. If the adversary can correlate ξ certificates of the interested vehicle, the tracing analysis succeeds. Let SP denote the success traceability probability. When the RSU is in secure state, the adversary has to find out every certificate of the interested vehicle from λ certificates at each time slot. Therefore, $\mathrm{SP} = 1/\lambda^{\xi}$. In PASS, when the RSU is compromised, the adversary can get no useful information; thus, $\mathrm{SP}_{\mathrm{PASS}} = \mathrm{SP}$. In ECPP, the adversary can directly find out the pseudonymous certificates of the interested vehicle; thus, $\mathrm{SP}_{\mathrm{ECPP}} = 1$. In DCS, the adversary has to confirm just one certificate of the interested vehicle; thus, $\mathrm{SP}_{\mathrm{DCS}} = 1/\lambda$. Given $\xi = 10$, Fig. 4 plots the success traceability probability versus the vehicle numbers in the region. It can be seen that PASS provides the best privacy preservation.

VII. Performance Evaluation

In this section, we evaluate the performance of the proposed PASS with the BP, ECPP, DCS, and Hybrid schemes. The classical public key infrastructure digital signature approach, i.e., the elliptic curve digital signature algorithm [23], is adopted in BP. Suppose the vehicle inspection is an annul check [2] and that the certificate validity period $\Delta T = 1$ min [5], [8]. We consider the implementation of Tate pairing on a Miyaji–Nakabayashi–Takano curve [25] with embedding degree 6, where $\mathbb{G}$ is represented by 161 bits, and the order q is represented by 160 bits. Moreover, the used hash function $h(.)$ is SHA-1. This way, Tables IV and V give the corresponding size in bytes for the certificates presented in this paper. Let T_{mul} denote the time to perform one point multiplication in $\mathbb{G}$, and let T_{par} denote the time of a pairing operation. Since T_{mul} and T_{par} dominate the speed of message signing and signature verification, we only consider these operations to evaluate all anonymous authentication schemes. For simplicity, the vehicles and RSUs are supposed to equip an Intel Pentium IV 3.0-GHz machine and run the same implementation of Tate pairing in [25]. Then, the following simulation adopts the measured processing time in [25], i.e., $T_{\mathrm{mul}} = 0.6$ ms and $T_{\mathrm{par}} = 4.5$ ms.

TABLE IV
Size of RSU and TA Signing Certificates. (a) RSU Certificate. (b) TA Signing Certificate

(a)

parameter	size in bytes
PK_{R_x}	21
D_y	4
σ_{TA,R_x}	42
total	67

(b)

parameter	size in bytes
$PK_{TA,V_i,k}$	21
$VP_{TA,V_i,k}$	4
$PID_{TA,V_i,k}$	20
$\sigma_{TA,TA,V_i,k}$	21
total	66

TABLE V
Size of Vehicle Pseudonymous Certificates. (a) Issued by the TA. (b) Issued by RSU R_x

(a)

parameter	size in bytes
$PK_{V_i,j}$	21
$VP_{V_i,j}$	4
$PID_{V_i,j}$	20
$\sigma_{TA,V_i,j}$	21
total	66

(b)

parameter	size in bytes
$PK_{V_i,j}$	21
$VP_{V_i,j}$	4
$PID_{V_i,j}$	20
$\sigma_{R_x,V_i,j}$	63
Cert_{TA,R_x}	67
total	175

A. Revocation Overhead

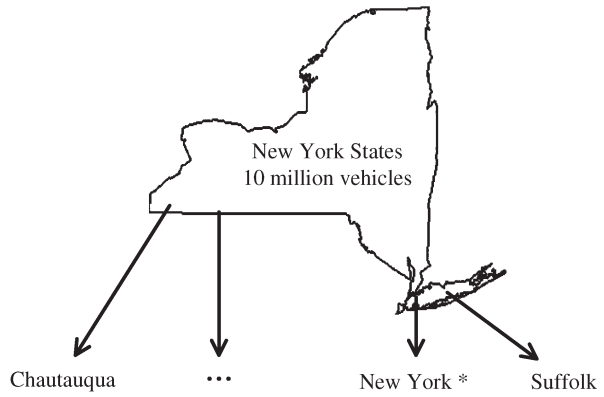
1) Updated CRL Size: The updated CRL will be transmitted to all vehicles by vehicle-to-vehicle communication. The smaller the CRL, the better it is for the VANET.

Table VI presents the CRL size to revoke one vehicle. In BP, ECPP, and DCS, all the pseudoidentities of unexpired certificates belonging to the revoked vehicle should be added into the CRL. Since the maximal size of the short-time pseudonymous certificate set in both ECPP and DCS is L_w, the average number of unexpired certificates is $(L_w + 1)/2$. In PASS, two hash seeds and the corresponding time window numbers will be added into the CRL, whereas the secret key of the revoked vehicle should be disclosed in Hybrid. Thus, the CRL size in PASS and Hybrid is constant.

The number of revoked vehicles is another important factor for the updated CRL size. The revocation ratio (denoted α) is defined as the ratio between the number of revoked vehicles every minute and the total number of vehicles. Suppose the TA is in charge of New York state, where there are about 10 million vehicles with active registrations according to the statistics of

TABLE VI
CRL SIZE FOR REVOKING ONE VEHICLE

method	unit size	item number	total (in bytes)
BP	21	48830	1025430
ECPP	21	$(L_w+1)/2$	$10.5*(L_w+1)$
DCS	8	$(L_w+1)/2$	$4*(L_w+1)$
Hybrid	21	1	21
PASS	48	1	48



*This region consists of Bronx, Kings, New York, Queens, and Richmond, and has 2 million registered vehicles.

Fig. 5. Domain distribution in New York state.

the New York State Department of Motor Vehicles [26], and the revocation ratio is uniform among the vehicles. Thus, $\alpha * 10^7$ vehicles would be revoked every minute in the whole precinct. In BP and Hybrid, the TA should publish a CRL of all these revoked vehicles. In ECPP, DCS, and PASS, the TA can divide the whole area to serval domains with the deployment of RSUs, as shown in Fig. 5. The CRL in each domain just contains the revoked membership in its own region. For example, New York City consists of Bronx, Kings, New York, Queens, and Richmond counties and has 2 million registered vehicles. Supposing that the real traffic in this region is about $2*(1+20\%)$ million vehicles, $\alpha * 2.4 * 10^6$ vehicles may be revoked in 1 min in this domain. Fig. 6 shows the size of the updated CRL in 30 min in New York City when the revocation ratio α varies from 0 to 10^{-7}. Through the comparison between BP, ECPP, DCS, and PASS and the comparison between Hybrid and PASS, it can be seen that the distribute certificate service nicely reduces the CRL size. Furthermore, the CRL size in ECPP and DCS depends on the RSU density, and three conditions, such as $L_w = 1$, $L_w = 60$, and $L_w = 120$, are presented. Obviously, if the RSUs are widely deployed, i.e., $L_w = 1$, DCS has the smallest CRL. Otherwise, PASS performs better.

2) Overhead for Revocation Checking: Revocation checking should run before certificate verification and is a part of entity authentication. The summary of the checking cost is given in Table VII.

In pseudonymous authentication schemes such as BP, ECPP, DCS, and PASS, when a vehicle receives a message signed by an unknown certificate, it checks the certificate pseudoidentity against the CRL. The efficiency of revocation checking depends on the string search algorithm. Supposing that they all use a hash map, the search algorithm takes $O(1)$ iterations [8]. Since the unit operation consists of a hash mapping (denoted $T_{\rm hash}$) and a string comparison (denoted $T_{\rm str}$), the total overhead can be omitted for message authentication. In the group-signature-based scheme Hybrid, the checking operation against one item in the CRL needs two pairing operations. Given the CRL with the size of $N_{\rm crl}$, the whole cost is $2N_{\rm crl}T_{\rm par}$. It can be seen that the revocation checking cost for 20 received messages/s can easily overcome 1 s if $N_{\rm crl}$ is larger than 6.

B. Certificate Updating Overhead

In this section, we compare the V2R communication overhead and the computation overhead for an RSU to handle a certificate updating request in ECPP, DCS, and PASS.

In PASS, the information exchanged between a vehicle and an RSU includes the RSU certificate, the encrypted signing certificate, the hint of secret key, and the re-signature key. Thus, the total communication overhead is 175 bytes. To serve a request, the RSU should compute the shared secret key and the re-signature key and verify the signing certificate. Thus, the computation cost is $4T_{\rm mul}$. In ECPP and DCS, a vehicle should require L_w pseudonymous certificates from an RSU. The overhead summary is given in Table VIII. It can be seen that PASS has the smallest communication overhead, which is independent from L_w, whereas the larger the certificate number L_w, the more service burden an RSU in ECPP and DCS has.

Furthermore, according to the computation overhead for handling a request, as shown in Table VIII, Fig. 7 shows the maximum number of requests that an RSU can serve per second versus L_w, where the RSU is assumed to be equipped with an Intel Pentium IV 3.0-GHz machine. It can be seen that PASS has the largest service capacity and performs much better than ECPP and DCS. Given $L_w = 60$, an RSU in ECPP can handle only one request, whereas it can solve less than six requests in DCS. In other words, when L_w increases, the RSUs can be inclined to be overloaded or be compromised by a DoS attack in ECPP and DCS.

C. Authentication Overhead

In this section, we analyze the overhead of authentication in three aspects: 1) communication overhead; 2) message-signing cost; and 3) message-verification cost.

1) Communication Overhead: Compared with the original traffic message, the attached certificate and signature can be recognized as extra communication overhead. In PASS, since the pseudonymous certificate issued by an RSU is 175 bytes and the Schnorr signature is 42 bytes, the communication overhead for a signed message is 217 bytes. The overhead summary for BP, ECPP, DCS, and Hybrid can be found in the second column in Table IX. BP achieves the smallest overhead because the vehicle certificates are directly issued by the TA. In the other schemes, a pseudonymous certificate has to embody a credential of the certificate's issuer so that the certificate size increases.

As discussed in Section V-F, it is efficient to broadcast a pseudonymous certificate once for K messages. This way, the average overhead for a signed message in PASS decreases to $175/K + 63$ bytes. Similarly, the overheads of the other

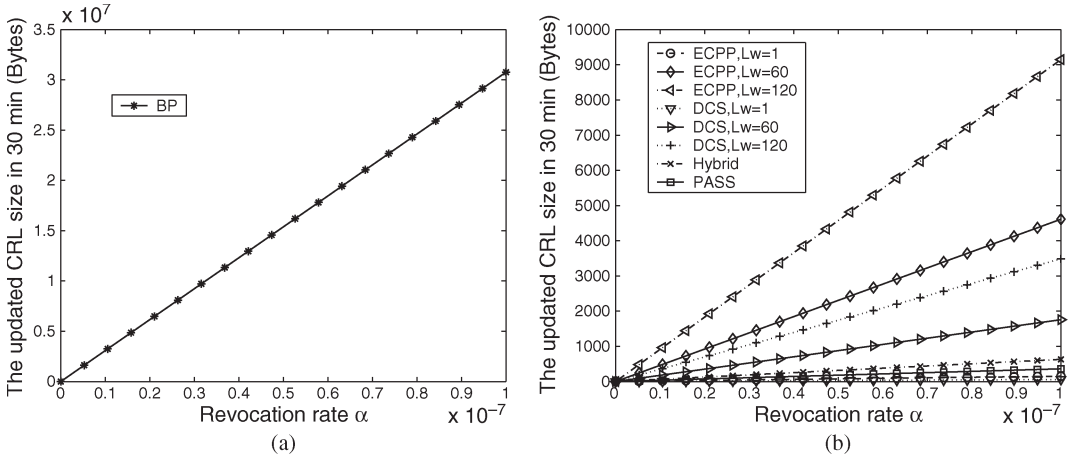


Fig. 6. Size of the updated CRL in 30 min in New York region.

TABLE VII
REVOCATION CHECKING OVERHEAD FOR ONE MESSAGE

method	unit operation	iterations	total
BP, ECPP, DCS, and PASS	T_{hash}+T_{str}	O(1)	0
Hybrid	$2T_{par}$	N_{crl}	$2N_{crl}T_{par}$

TABLE VIII
OVERHEAD FOR HANDLING ONE REQUEST

Method	Communication Overhead	Computation Overhead
ECPP	105+147L_w	(3+2L_w)T_{par}+ (4+9L_w)T_{mul}
DCS	270+84L_w	5T_{par}+(2+4L_w)T_{mul}
PASS	175	4T_{mul}

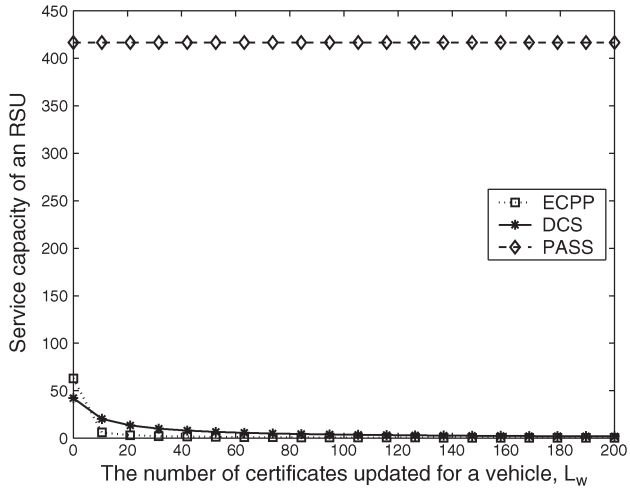


Fig. 7. Maximum number of requests that an RSU can serve per second.

TABLE IX
COMMUNICATION OVERHEAD OF MESSAGE AUTHENTICATION

method	original format	one certificate for K messages ($K > 1$)
BP	105	$63/K + 63$
ECPP	189	$147/K + 63$
DCS	209	$167/K + 63$
Hybrid	189	$147/K + 63$
PASS	217	$175/K + 63$

schemes are given in the last column in Table IX. When K increases, the overhead is closer to 63 bytes, which is the total size of a public key and a signature.

TABLE X
COST FOR SIGNING AND VERIFICATION

method	signing	certificate verification	signature verification
BP	T_{mul}	$2T_{mul}$	$2T_{mul}$
ECPP	T_{mul}	$3T_{par}$+$9T_{mul}$	$2T_{mul}$
DCS	$2T_{mul}$	$3T_{par}$+$2T_{mul}$	$3T_{par}$+T_{mul}
Hybrid	T_{mul}	$2N_{crl}T_{par}$+$3T_{par}$+$9T_{mul}$	$2T_{mul}$
PASS	T_{mul}	$3T_{par}$+$2T_{mul}$	$2T_{mul}$

2) Message-Signing Cost: In PASS, a vehicle adopts the Schnorr signature algorithm to sign the messages. The cryptography operation involves a point multiplication; thus, the signing overhead is $T_{\rm mul}$. The delay is so small that there is no loss of the information accuracy of a routine traffic message. For example, supposing that the speed of a vehicle is 15 m/s, its location may change less than 1 mm after the message has been signed. The second column in Table X gives the signing cost for BP, ECPP, DCS, Hybrid, and PASS. It can be seen that all these schemes are feasible.

3) Message-Verification Cost: The message-verification cost consists of certificate verification and signature verification. Before verifying a vehicle certificate, revocation checking must run if the local CRL is not empty. As discussed in Section V-E, the checking cost can be omitted in the pseudonymous authentication schemes, whereas it must be accounted for in group-signature-based schemes such as Hybrid. Therefore, the certificate verification overhead in PASS depends on the cost for verifying an RSU certificate and the RSU's signature in the vehicle certificate, which takes three pairing operations and two point multiplications. Therefore, the certificate-verification cost is $3T_{\rm par} + 2T_{\rm mul}$. In addition, verifying a message signature needs two point multiplications; thus, the cost is $2T_{\rm mul}$. The overhead summary for the other schemes can be found in Table X. Notice that the certificate-verification overhead of Hybrid involves the revocation checking cost $2N_{\rm crl}T_{\rm par}$.

It can be seen that BP has the lowest certificate-verification cost because its pseudonymous certificate is directly signed by the TA, and DCS and PASS have the second lowest overhead. Moreover, PASS gives the lowest signature overhead, as does BP. Using the public key buffer, a vehicle just needs to verify a valid certificate once, whereas signature verification

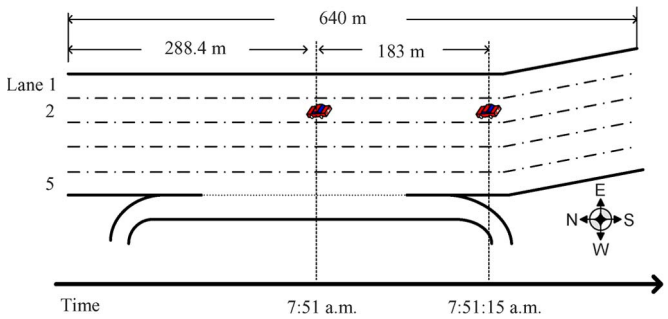


Fig. 8. Southbound direction of U.S. Highway 101 in Los Angeles, CA.

TABLE XI
NS-2 SIMULATION PARAMETERS

parameter	value
simulation area length	640m
simulation time	15 sec
vehicle density	18 vehicles/100m
average vehicle speed	12.54 m/sec
transmission range	300 m
MAC protocol	802.11
channel bandwidth	6 Mbps

is necessary for every received message. Therefore, signature verification dominates the message-authentication efficiency after most of the certificates of the neighboring vehicles have been verified. Then, PASS can perform the best, as does BP.

To further evaluate the authentication efficiency, we conduct ns-2 simulation [27] using the real vehicle trajectory data on southbound U.S. Highway 101 (Hollywood Freeway) in Los Angeles, CA, on June 15, 2005, which was provided by the Next Generation Simulation (NGSIM) project [28]. As shown in Fig. 8, the study area is approximately 640 m in length and consists of five lanes and an auxiliary lane. The adopted simulation parameters are given in Table XI. We use the vehicle trajectory data of the period from 7:51 AM to 7:51:15 AM when the most part of the communication range of the selected vehicle in the second lane is in the study area. According to DSRC, each vehicle has to disseminate a routine traffic message every 300 ms. Without loss of generality, suppose 5% of vehicles act as misbehaving members and broadcast two fake messages every 300 ms. One fake message attaches a bogus certificate, and the other message attaches a bad signature. Considering that the traffic information rapidly varies, the vehicles would drop the messages that cannot be verified every 300 ms. The message loss ratio is defined as the ratio between the number of messages dropped every 300 ms and the total number of messages received every 300 ms. Notice that DCS supports batch verification for certificates and signatures, which is more efficient than verifying them separately when there is no fake messages. To evaluate the DCS when it adopts the batch verification strategy (denoted DCS_batch), we use the average overhead of message verification based on binary authentication tree [13], i.e.,

$$5\left(\frac{(N_f+1)}{N_m}\lg\left(\frac{N_m}{N_f}\right)+\frac{4N_f-2}{N_m}\right)T_{\text{par}}+3T_{\text{mul}}$$

where N_f is the number of fake messages ($N_f \geq 1$) every 300 ms, and N_m is the total number of received messages every 300 ms. Moreover, two conditions, i.e., $N_{\text{crl}}=0$ and $N_{\text{crl}}=50$, in Hybrid are observed. Fig. 9 shows the simulated message loss ratios at each 300 ms for BP, ECPP, DCS, DCS_batch, Hybrid, and PASS, respectively. It can be seen that BP performs the best due to the lowest authentication overhead, and the performance of PASS is almost close to BP. At the initial stage of simulation, the vehicles in PASS have no idea on which certificates are veritable and have to verify both of the certificate and the message signature for the received messages. They cannot afford so much overhead, and some messages will be dropped. As the number of verified certificates increases in the following stages of simulation, the message-verification overhead is only contingent upon the signature verification; thus, PASS performs as efficiently as BP. With the same reasons, the message loss ratios in ECPP, DCS, and Hybrid are also large at the beginning and reduce during the running of the simulation. Because the certificate verification cost is high in DCS and Hybrid, and the number of received bogus certificates varies every 300 ms, the message lost ratios in them do not monotonously decrease. Moreover, we can observe that DCS_batch also does not work well because batch verification is not efficient once the fake messages exist.

D. Storage Overhead for a Vehicle

In PASS, a vehicle obtains $C*L_w$ secret keys, $C*L_w$ pseudonymous certificates, and C signing certificates from the TA, which dominate the storage overhead. According to the certificate size given in Tables IV and V, we can obtain the storage overhead

$$\text{Stor}=C*L_w*21+C*L_w*66+C*66.$$

Suppose all vehicles can pass through an RSU within 60 min. Thus, $L_w=60$, and $C=24*365=8760$. Therefore, the storage overhead Stor $=4605360$ bytes ≈ 45 Mb, which is acceptable for the current storage capacity.

VIII. CONCLUSION

In this paper, we have proposed PASS for secure vehicular communications. PASS cannot only satisfy the security and privacy requirements of VANETs but can also significantly reduce the revocation cost and the certificate updating overhead. Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries cannot trace the legitimate vehicles, although they have compromised all RSUs. For our future work, we will investigate the location privacy issue under the context of the proposed PASS scheme.

ACKNOWLEDGMENT

The authors would like to thank X. Liang, Q. Hu, B. Zhao, and the anonymous reviewers for their helpful comments.

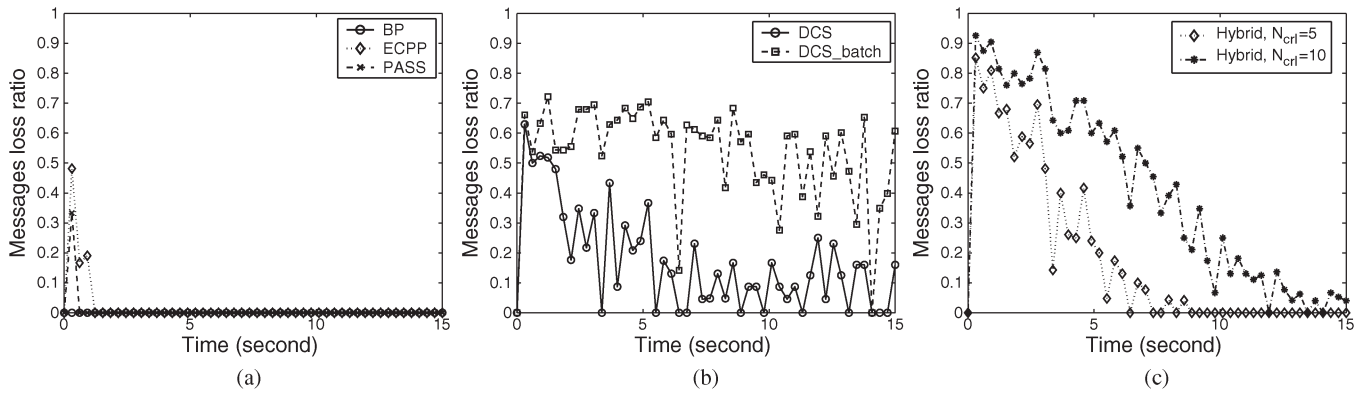


Fig. 9. Comparison between message loss ratios for different schemes.

REFERENCES

[1] Dedicated Short Range Communications (DSRC) Home. [Online]. Available: http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[2] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. HotNets-IV*, Nov. 2005, pp. 1–6.

[3] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A new VANET-based smart parking scheme for large parking lots," in *Proc. INFOCOM*, Rio de Janeiro, Brazil, Apr. 2009, pp. 1413–1421.

[4] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. INFOCOM*, San Diego, CA, Mar. 2010, pp. 1–9.

[5] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[7] J. Guo, J. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. Mobile Netw. Veh. Environ.*, Anchorage, AK, May 2007, pp. 103–108.

[8] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. 4th ACM Int. Workshop VANET*, Montreal, QC, Canada, 2007, pp. 19–28.

[9] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. INFOCOM*, Phoenix, AZ, Apr. 2008, pp. 1229–1237.

[10] B. Bellur, "Certificate assignment strategies for a PKI-based security architecture in a vehicular network," in *Proc. IEEE GLOBECOM*, New Orleans, LA, Nov. 2008, pp. 1–6.

[11] C. Jung, C. Sur, Y. Park, and K. Rhee, "A robust conditional privacy-preserving authentication protocol in VANET," in *Proc. MobiSec*, Turin, Italy, Jun. 2009, pp. 35–45.

[12] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed certificate service scheme for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 533–549, Feb. 2010.

[13] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1974–1983, Apr. 2009.

[14] K. Laberteaux, J. Haas, and Y. Hu, "Security certificate revocation list distribution for VANET," in *Proc. 5th ACM Int. Workshop VANET*, San Francisco, CA, 2008, pp. 88–89.

[15] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *Proc. 5th ACM Int. Workshop VANET*, San Francisco, CA, 2008, pp. 86–87.

[16] B. Libert and D. Vergnaud, "Multi-use unidirectional proxy re-signatures," in *Proc. ACM CCS*, Alexandria, VA, Oct. 2008, pp. 511–520.

[17] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. ACM CCS*, 2004, pp. 168–177.

[18] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. IEEE WCNC*, Mar. 2005, pp. 1187–1192.

[19] J. Freudiger, M. Raya, M. Feleghhazi, P. Papadimitratos, and J.-P. Hubaux, "Mix zones for location privacy in vehicular networks," in *Proc. WiN-ITS*, Aug. 2007, pp. 1–7.

[20] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1569–1589, Oct. 2007.

[21] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Adv. Cryptology—CRYPTO*, vol. 2139, *LNCS*, 2001, pp. 213–229.

[22] C.-P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptology*, vol. 4, no. 3, pp. 161–174, Jan. 1991.

[23] W. Mao, *Modern Cryptography: Theory and Practice*. Englewood Cliffs, NJ: Prentice-Hall, 2003.

[24] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptology*, vol. 17, no. 4, pp. 297–319, Sep. 2004.

[25] M. Scott, *Efficient Implementation of Cryptographic Pairings*. [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf

[26] The New York State Department of Motor Vehicles, *NYS DMV—Statistics—Vehicle Registrations in Force—2008*. [Online]. Available: http://www.nysdmv.com/Statistics/regin08.htm

[27] *The Network Simulator–ns-2*. [Online]. Available: http://nsnam.isi.edu/nsnam/index.php/

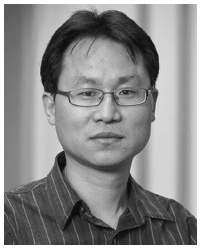
[28] *The Next Generation Simulation (NGSIM) Program*. [Online]. Available: http://www.ngsim.fhwa.dot.gov/

Yipin Sun (S'09) is currently working toward the Ph.D. degree with the School of Computer Science, National University of Defense Technology, Changsha, China.

Between September 2008 and September 2009, he was with the Broadband Communications Research Group, University of Waterloo, Waterloo, ON, Canada. His research interests include intrusion detection, network security, and applied cryptography.

Rongxing Lu (S'09) is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

He is currently a Research Assistant with the Broadband Communications Research Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.



Xiaodong Lin (S'07–M'09) received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008.

He is currently an Assistant Professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON. His research interests include wireless network security, applied cryptography, computer forensics, and software security.

Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada Canada Graduate Scholarships Doctoral Award and the Best Paper Award at the 2009 IEEE International Conference on Computer Communications and Networks and the 2007 IEEE International Conference on Communications—Computer and Communications Security Symposium.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree in electrical engineering from Dalian Maritime University, Dalian, China, in 1982 and the M.Sc. and Ph.D. degrees in electrical engineering from Rutgers University, Camden, NJ, in 1987 and 1990, respectively.

He is currently a Professor and the University Research Chair with the Centre for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He is a coauthor of three books and has published more than 400 papers and book chapters on wireless communications and networks, control, and filtering. He serves as the Editor-in-Chief for *Peer-to-Peer Networking and Application* and an Associate Editor for *Computer Networks*, *ACM/Wireless Networks*, and *Wireless Communications and Mobile Computing*. He has also served as a Guest Editor for *ACM Mobile Networks and Applications*. His research focuses on resource management in interconnected wireless/wired networks, ultrawideband wireless communications networks, wireless network security, wireless body area networks, and vehicular ad hoc and sensor networks.

Dr. Shen is a Registered Professional Engineer in the Province of Ontario and a Distinguished Lecturer of the IEEE Communications Society. He has served as the Technical Program Committee Chair for the 2010 IEEE Vehicular Technology Conference; the Tutorial Chair for the 2008 IEEE International Conference on Communications; the Technical Program Committee Chair for the 2007 IEEE Global Telecommunications Conference; the General Cochair for the 2007 International Conference in Communications and Networking in China and the 2006 International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks; and the Founding Chair for the IEEE Communications Society Technical Committee on Peer-to-Peer Communications and Networking. He has also served as a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and the KICS/IEEE JOURNAL OF COMMUNICATIONS AND NETWORKS. He has also served as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS, and the *IEEE Communications Magazine*. He was the recipient of the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo; the Premier's Research Excellence Award in 2003 from the Province of Ontario; and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo.

Jinshu Su (M'05) received the B.S. degree in mathematics from Nankai University, Tianjin, China, in 1985 and the M.S. and Ph.D. degrees in computer science from the National University of Defense Technology, Changsha, China, in 1988 and 2000, respectively.

He is a Professor with the School of Computer Science, National University of Defense Technology. His research interests include Internet architecture, Internet routing, security, and wireless networks. He currently leads the Distributed Computing and High Performance Router Laboratory and the Computer Networks and Information Security Laboratory, which are both key laboratories of National 211 and 985 projects, China. He also leads the High Performance Computer Networks Laboratory, which is a key laboratory of Hunan Province, China.