ECPB: Efficient Conditional Privacy-Preserving Authentication Scheme Supporting Batch Verification for VANETs

Yimin Wang[1,2], Hong Zhong[1], Yan Xu[1] and Jie Cui[1]
(Corresponding Author: Hong Zhong)
School of Computer Science and Technology, Anhui University[1]
Hefei 230601, China
Modern Education and Information Center, Anhui Agriculture University[2]
Hefei 230036, China
(Email: ymwang@ahu.edu.cn)
(Received May 12, 2015; revised and accepted July 2 & July 13, 2015)

Abstract

In this paper, we introduce an efficient Conditional Privacy-Preserving authentication scheme(ECPB) based on group signature for vehicular ad hoc networks (VANETs). Although group signature is widely used in VANETs for security requirements, the existing schemes based on group signatures suffer longer computational delays in the certificate revocation list (CRL) checking and in the signature verification process, leading to lower verification efficiency. In our scheme, membership validity (a validity period) is required when a vehicle applies for a group member and this validity is used to check whether the vehicle is still a group member or not, which can be used as a substitute for the CRL checks. Neglecting the CRL checks will sharply decrease the costs incurred in the signatures verification. In addition, our proposed scheme also supports batch verification. Experimental analysis proves that our proposed scheme exhibit improved efficiency over the existing schemes, in terms of verification delay and average delay.

Keywords: Batch verification, CRL, group membership validity, group signature, VANETs

1 Introduction

In vehicular ad hoc networks (VANETs) is a subset of mobile ad hoc networks (MANETs), which uses mobile vehicles as network nodes in order to enable communication. Such network nodes include both onboard units (OBUs) those equipped with in mobile vehicles and road side units (RSUs) those mounted on stable units (traffic posts etc.). These network nodes communicate among each other to so that they can access the application server for retrieving services. In general, services provided via VANETs include traffic information for drivers, such as traffic accident, traffic condition, weather forecast and multimedia infotainment dissemination, etc. [8], thus helps improving driving safety. One of the prevailing issues in the design of VANETs is the anonymous authentication being involved whilst disseminating messages. In general, users tend to protect their identity and location during the authentication process.

However, such anonymous message authentication in VANETs should be conditional, in a way that, trusted authorities should be able to track the vehicles involved in their targeted path, enabling them to collect the safety messages during dissemination. But, such a scenario creates conflicts between privacy and accountability. To this end, existing methods in solving this conditional privacy issues in VANETs include pseudonym-based scheme and group-oriented signature-based scheme etc. Pseudonym-based scheme [7] uses a pseudonym irrelevant to the real identity of the senders for the purpose of protecting their privacy in the communication process. But in practice, such an irrelevant identity for the senders can hardly be achieved by one pseudonym whilst disseminating multiple messages, thus demanding pre-packaged massive pseudonyms [3]. And each pseudonym has a corresponding certificate to ensure its legitimacy. Besides, anonymity in VANETs requires that adversaries cannot connect the newly generated pseudonyms with the previous ones whenever vehicles update the pseudonyms. In order to improve the efficiency of the authentication process, the proposed b-SPECS+ scheme [6] is a pseudonym-based approach incorporated with a batch Verification process. Genetically, pseudonym schemes include several drawbacks, exhibiting flaws in their storage structure, certificate issuing mechanisms and update strategies. Also, such schemes demand massive storage space

for the pseudonyms and incur high costs for newly acceded vehicles in the communication path and exhibit low query efficiency.

Group-oriented signature-based scheme [1] is widely used in VANETs for vehicles to achieve anonymous authentication [4, 10, 19], as it is capable of eliminating the inefficiencies of the Pseudonym-based approach. According to Calandriello et al. [12], group-oriented signature-based scheme with public key infrastructure (PKI) is better than other methods in computing and storage efficiency, based on their analysis on signature and verification process. But, the major disadvantage of the group-oriented signature-based scheme is the overheads involved in the CRL (checking, storing and updating, etc) process. If a vehicle is revoked, it will be added into the CRL. Thus when receiving a message from an unknown entity, a vehicle has to check the CRL to avoid communicating with revoked vehicles and then verify the senders group signature to check the validity of the received message. This approach generally requires 9 ms to check one identity in the CRL, To expand on that, for n revoked identities in the CRL, the number of messages that can be verified in one second is $1000/(9n + 1)$, which is far smaller than the requirement of 600 in VANETs [17]. The CRSB protocol [16], introduced by Zeng et al., is based on ring signature (ring signature can be regarded as simplified group signature) to verify the message, the time increases linearly as the number of revoked vehicles in the revocation list grows. Zhang et al. [18] applied batch group signature verification to improve the efficiency of the authentication process, Similar issue prevails in the method [15] proposed by Wasef et al. But, the two schemes can only verify 274 and 127 messages per second, respectively, which still cannot satisfy the requirement of verifying 600 messages per second. Hao et al. [5] proposed a novel distributed key management scheme based on cooperation among vehicles. Although this scheme can achieve the verification speed of 600 messages per second, it is not effective in eliminating the CRL checking overhead. Studer et al. [14] proposed the VAST scheme based on Elliptic Curve Digital Signature Algorithm (ECDSA) and Timed Efficient Stream Loss-Tolerant Authentication (TESLA++). VAST combines the advantages of ECDSA and TESLA++, where ECDSA provides fast authentication and non-repudiation, and TESLA++ guarantees data integrity. Still, this scheme does not consider anonymity and traceability. Lu et al. [13] proposed the SPRING scheme, which incorporates the Trust Authority (TA) framework to improve the overall efficiency. Because the whole scale of CRL will be decreased in this method when the shot-term certificates and the CRL are limited to single Road Side Units (RSUs). Based on the social degree information, SPRING places RSUs at high-social intersections to improve the communication efficiency. Due to the larger number of interacting protocols, this scheme incurs communication delays. Further, it exhibits a weaker privacy protection as the security of the entire process relies heavily on the RSU. Another strategy of improving privacy protection in VANETs is to use shared keys [11] as a substitute for anonymous certificates or pseudonyms to verify vehicle safety messages.

With this in mind, this paper proposes a novel communication protocol based on group signature to tackle the conditional privacy presentation and authentication for VANETs, called ECPB. Differing from the existing group signature based schemes, ECPB uses validity as a substitute for CRL checks. In other words, it is focused on rectifying problems caused by CRL, such as the overhead involved in storing, communication, updating and checking process.

Remark 1. *Unlike the existing schemes based on Pseudonym, our communication protocol(ECPB) does not require each vehicle to store a large number of keys and anonymous certificates, and so the storage overhead of our scheme is lower. Also ECPB guarantees anonymity and traceability, as it is based on group signature scheme, which is not found in VAST. Comparing to SPRING, ECPB does not require any RSUs for the purposes of authenticating messages, tracing the vehicles. Because of using the validity to be a substitute of checking CRL, it offers faster message authentication. While in CRSB, the time increases linearly as the number of revoked vehicles in the CRL grows when verifying messages. In addition, ECPB can support batch verification.*

Table 1 presents an overview of the security of our proposed scheme over other existing schemes. The remainder of this paper is organized as follows. Section 2 presents our system model and the security goals. Section 3 introduces the preliminaries of our approach. Section 4 proposes our scheme, and the security analysis and performance evaluation are discussed in Section 5. And Section 6 concludes this paper.

Table 1: Overview of the security of ECPB over existing schemes

	CRSB	**VAST**	**SPRING**	**Our Scheme**
Integrity	√	√	√	√
Non-repudiation	√	√	×	√
Privacy	√	×	√	√
Anonymity	√	×	√	√
Certificateless	√	×	×	√
Conditional traceability	√	×	√	√
Revocability	√	√	√	√
Efficient verification	×	√	√	√
Batch verification	×	×	×	√

2 System Model and Security Goals

In this section, we present the main entities and attributes of VANETs, illustrated in Figure 1. In addition, this section also presents the security requirements that should be satisfied during communications in VANETs.

2.1 System Model

The proposed system model of VANETs consists of a trust authority (TA), service providers (SP), RSU, OBU, as shown in Figure 1.

TA: a trusted third party, for example, the government traffic management department, acts as the management center of the network; it provides registration and certification (public key certificate, PKC) for vehicles and group manager when they join the network.

SP: service provider, the group manager in the model; the service is chargeable and the group member can pay for a period of validity and then he can use the service in the validity; whose main mission is to authenticate vehicles by providing them with the group public key and group members secrete key for signature and verification.

RSUs: infrastructure of VANETs, they act as the bridge between SP and OBUs or between two OBUs, connecting SPs by wire and connecting OBUs by a wireless channel respectively.

OBUs: a unit that is embedded in vehicles, is the indispensable basic entity in VANETs; this unit is similar to the mobile terminal of communication systems, the hardware security module of it ensures the security of calculation, such as encryption and decryption; and it is responsible for the communication of vehicles and RSU, and periodically broadcasts traffic-related status information.

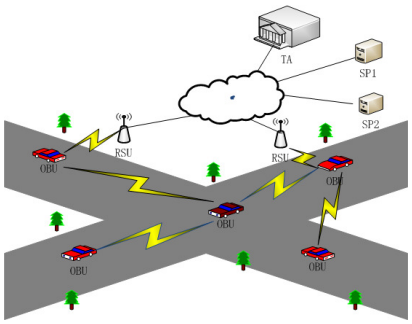

Figure 1: System model of VANETs

2.2 Security Goals

Authentication: Node authentication, helps users to ensure that the node identity information to which they establish communication is real.

Non-repudiation: Authenticated vehicles cannot deny messages after sending to the VANETs.

Anonymity: Other vehicles and adversaries in VANETs cannot identify the sender's identity.

Traceability: Manager of VANETs can identify the real identity of the senders for malicious and controversial messages.

Forward and backward security revocation: Vehicle cannot access the services both before authentication and after revocation; other vehicles cannot access the services as an impostor.

3 Preliminaries

In this section, we briefly introduce the statistical techniques used in our protocol.

Bilinear Pairing. Both G_1 and G_2 are two (multiplicative) cyclic groups of prime order q. g_1 is the generator of G_1, g_2 is the generator of G_2. ψ is a computable isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$. e is a bilinear map, and $e : G_1 \times G_2 \to G_T$, satisfies the following rules:

1) Bilinear: $e(ag_1, bg_2) = e(g_1, g_2)^{ab}$, for all $g_1 \in G_1, g_2 \in G_2$ and $a, b \in Z_q^*$.
2) Non-degenerate: $e(g_1, g_2) \neq 1$.
3) Computable: $e(g_1, g_2)$ is efficiently computable, and $e(g_1, g_2) = e(g_2, g_1)$.

Zero-knowledge Proof. Alice and Bob are two participants, and Alice has a secret M. Alice communicates with Bob to demonstrate that she has a secret but do not tell Bob any other messages of the secret. It means that Bob knows that Alice has a secret, but he does not know what the secret is.

Strong Diffie-Hellman Hypothesis. Let G_1, G_2 be cyclic groups of prime order p, where possibly $G_1 = G_2$. Let g_1 be the generator of G_1, g_2 be the generator of G_2. Given $(g_1, g_2, g_2^r, \ldots, g_2^{r_q})$ as input, output will be a pair $(g_1^{1/(r+x)}, x)$. In multiple-term formula time, it is unsolvable, and is called q-SDH.

4 Description of Our Scheme

Before the deployment of the message transmission, vehicle registration, SP registration and initialization of the whole protocol, including system parameter generation, are achieved by TA, as shown in Figure 2. For example,

every vehicle will achieve a unique identity V_{id} from TA during vehicle registration, including an electronic license, legal certificate $Cert_{V_{id}}$, and a pair of public and secrete key (V_{sk}, V_{pk}). Before providing services, SP submit an application to TA, and will obtain a unique identity S_{id}, legal certificate $Cert_{Si}$ and a pair of public and secrete key (S_{sk}, S_{pk}). The notations used in the following scheme are listed in Table 2.

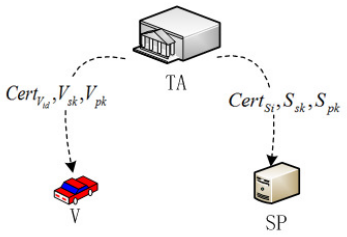

Figure 2: Vehicle and SP registration

Table 2: Notation and description

Notation	Description
TA	A trust authority
SP	Service provider
$Cert_{V_{id}}$	The certificate of V_{id}
$Cert_{Si}$	The certificate of S_{id}
V_{id}	The real identity of vehicle V from TA
V_{sk}, V_{pk}	A pair of public and secrete key of V
S_{id}	The real identity of Service provider S from TA
S_{sk}, S_{pk}	A pair of public and secrete key of S
M	The authenticated message
H, H_1, H_2	Hash function
$Sig(\cdot)$	Digital signature algorithm
$m\|n$	Concatenation of strings m and n

4.1 System Initialization

As the basis of the system group initialization, TA initiates the bilinear parameter $(G_1, G_2, G_T, e, g_1, g_2, q, \varphi, H)$, where e is a bilinear pair $G_1 \times G_2 \to G_T$, and all groups G_1,G_2,G_T are multiplicative cyclic groups of the prime order q. g_1 is the generator of G_1, g_2 is the generator of G_2, and $\varphi(g_2) = g_1$, Hash Function is $H : \{0,1\}^* \to Z_q^*$.

4.2 Operation of ECPB

This subsection details the operation of our scheme. The operation includes five parts such as membership application (Figure 3), membership registration (Figure 3), vehicle safe message generation, message verification (Figure 4), and traceability of controversial message.

In our scheme, Group signature key management system is managed by the SP as follows:

1) SP chooses random numbers $h \in G_1$ and $k_1, k_2 \in Z_q^*$, given $u^{k_1} = v^{k_2} = h$, where $u, v \in G_1$, thus all $g_1, u, v, h \in G_1$.

2) SP chooses hash function $H_1 : \{0,1\}^* \to Z_q^*$, uses the unique identity S_{id}, computes $r = H_1(S_{id})$ and $w = g_2^r$, then $g_2, w \in G_2$; and then chooses another hash function: $H_2 : \{0,1\}^* \to Z_q^*$.

SP provides group public parameter $\{u, v, h, w, H_2\}$, where the master key is $gmsk = (k_1, k_2)$, and the public key of the group signature system is $gpk = (g_1, g_2, h, u, v, w, H_2)$.

Figure 3: Group membership application and registration

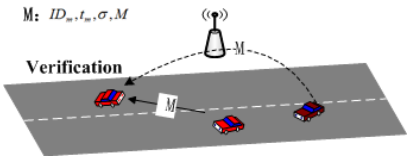

Figure 4: Message verification

Membership Application. SP broadcasts its service information $\{S_{pk}, Cert_{Si}, S_{id}, Sig_{S_{sk}}(S_{id})\}$, where S_{pk} is the public key, $Cert_{Si}$ is the PKC, S_{id} is its unique identity, $Sig_{S_{sk}}(S_{id})$ is its signature. When a vehicle receives a message, it executes it as follows:

1) The vehicle identifies the legality of S_{pk} through its $Cert_{Si}$, then verifies the validity of $Sig_{S_{sk}}(S_{id})$ by using S_{pk} to confirm that the message source is real, not falsifying.

2) The vehicle sends its application information $\{V_{pk}, Cert_{Vi}, V_{id}, Sig_{V_{sk}}(V_{id}), T_i\}$ to SP, where V_{pk} is the public key of the vehicle, $Cert_{Vi}$ is the PKC, V_{id} is its unique identity, $Sig_{V_{sk}}(V_{id})$ is the signature, and T_i is the membership validity.

Membership Registration. Receiving an application message from a vehicle, the operations of SP are illustrates as follows:

1) SP identifies the legality of V_{pk} through $Cert_{Vi}$, and then verifies the validity $Sig_{V_{sk}}(V_{id})$ by using V_{pk} to confirm that the message source is real, not falsifying.

2) SP selects a random number v_i, computes $x_i = H_1(V_{id}\|v_i)$, gives $f_i = g_1^{1/(x_i+r)}$, then chooses a random number s_i, computes $s_i' = H_2(s_i)$, then computes $t_i = H_2(T_i\|s_i')$, and gives $f_i' = (f_i)^{t_i}$

as the group identity information of the vehicle, which establishes the corresponding relationship with V_{id}, and stores it. The group membership secrete key of the vehicle is $gsk[i] = (x_i, f_i{}', s_i)$, and it encrypts $E_{v_{pk}}(x_i, f_i{}', s_i)$ by its public key V_{pk}, then sends it to vehicle V_{id}.

Vehicle Safe Message Generation. Each vehicle in VANETs generates the signature on message $M \in \{0,1\}^*$ before sending it. In our scheme, we take a common vehicle who has become a group member which obtain $gpk = (g_1, g_2, h, u, v, w, H_2)$ and $gsk[i] = (x_i, f_i{}', s_i)$ by decrypting $E_{v_{pk}}(x_i, f_i{}', s_i)$ using the vehicles secrete key V_{sk}. Before sending a message $M \in \{0,1\}^*$, the message will be signed. In this message generation, the signature σ is computed as follows:

1) The vehicle checks the validity of T_i. If T_i is invalid, then the vehicle sends a new application to SP for a group member. If it is valid, it will compute $s_i{}' = H_2(s_i)$ initially and then computes $t_i = H_2(T_i \| s_i{}')$.

2) The vehicle selects random numbers α, β, r_α, r_β, r_x, r_{γ_1}, $r_{\gamma_2} \in Z_q$ and computes:

$$A_1 = u^\alpha; A_2 = v^\beta; A_3 = f_i{}' \cdot h^{\alpha+\beta};$$
$$\gamma_1 = x_i \cdot \alpha; \gamma_2 = x_i \cdot \beta;$$
$$R_1 = u^{r_\alpha}; R_2 = v^{r_\beta};$$
$$R_3 = e(A_3, g_2)^{r_x} \cdot e(h, w)^{-r_\alpha - r_\beta} \cdot e(h, g_2)^{-r_{\gamma_1} - r_{\gamma_2}};$$
$$R_4 = A_1^{r_x} \cdot u^{-r_{\gamma_1}}; R_5 = A_2^{r_x} \cdot u^{-r_{\gamma_2}};$$

Then it computes:
$\lambda = H(M, A_1, A_2, A_3, R_1, R_2, R_3, R_4, R_5)$.

3) The vehicle gives $\lambda' = \lambda / t_i$, then computes.

$$s_\alpha = r_\alpha + \lambda' \cdot \alpha; s_\beta = r_\beta + \lambda' \cdot \beta; s_x = r_x + \lambda' \cdot x;$$
$$s_{\gamma_1} = r_{\gamma_1} + \lambda' \cdot \gamma_1; s_{\gamma_2} = r_{\gamma_2} + \lambda' \cdot \gamma_2;$$

Based on the above computations, signature σ of M is $(A_1, A_2, A_3, \lambda, s_\alpha, s_\beta, s_x, s_{\gamma_1}, s_{\gamma_2}, s_i{}', T_i)$. Now M and σ are broadcasted, and the concrete format of broadcasted message is shown in Table 3.

Table 3: Formats of broadcast message

Message Identifier	Timestamp	Signature	Message
ID_m	t_m	σ	M

Message Verification. Based on the strong Diffie-Hellman Assumption, group member authenticates a signature by using the zero-knowledge proof. It means that without the identity $f_i{}'$ and other secrete information of the sender, such as x_i, s_i, verifiers can validate the legality of the senders. In order to prevent a message from replay attacks, the freshness of t_m is verified upon receiving the corresponding message, as illustrated in Algorithm 1.

Algorithm 1 Message Verification

Require: $gpk = (g_1, g_2, h, u, v, w, H_2), M, \sigma = (A_1, A_2, A_3, \lambda, s_\alpha, s_\beta, s_x, s_{\gamma_1}, s_{\gamma_2}, s_i{}', T_i)$.

```
Begin
if T_i is invalid then
    Drop the message;
else
    Compute: t_i = H_2(T_i || s_i');
    Set λ' = λ/t_i
    Compute:
    R_1 = A_1^{-λ'} · u^{s_α}
    R_2 = A_2^{-λ'} · v^{s_β}
    R_3 = e(A_3, g_2)^{s_x} · e(h, w)^{-s_α - s_β} · e(h, g_2)^{-s_{γ1} - s_{γ2}}
    ·(e(A_3, w)^{1/t_i} / e(g_1, g_2))^{λ}
    R_4 = A_1^{s_x} · u^{-s_{γ1}}
    R_5 = A_2^{s_x} · v^{-s_{γ2}}
    Verify:
    λ ?= H(M, A_1, A_2, A_3, R_1, R_2, R_3, R_4, R_5)
    if true then
        Accept M;
    else
        Drop the message;
    end if
end if
End
```

Traceability of Controversial Message. Upon receiving a controversial message, it is necessary to find out the real identity of the sender. The group manager will first verify whether the sender's M and σ are real and correct, similar to the verification process of Algorithm 1. Then, using the master key $gmsk = (k_1, k_2)$, the real identity $A_3/(A_1^{k_1} \cdot A_2^{k_2}) = f_i{}'$ of the sender is computed, thereby identifying the corresponding vehicle V_{id} from the storage list.

4.3 Batch Verification

Our proposed scheme supports batch verification, which helps improving the signature verification efficiency. Now, R_3 has been given in the new signature $Sig_n(M)$ in advance, so it just needs to be verified and not to be calculated. Suppose that a vehicle receives n messages, the batch verification process of the traffic messages is executed as shown in Algorithm 2($\tau_1, \ldots, \tau_n$ is random vector, and $\tau_j \in Z_q$). Successful completion of this batch verification allows the validation of n messages together.

$$Sig_n(M_j) = (A_{j,1}, A_{j,2}, A_{j,3}, R_{j,3}, \lambda_j, s_{j,\alpha}, s_{j,\beta}, s_{j,x}, s_{j,\gamma_1}, s_{j,\gamma_2}, s_j{}', T_j), 1 \le j \le n.$$

Algorithm 2 Batch Verification

Require: $gpk = (g_1, g_2, h, u, v, w, H_2)$, M, $Sig_n(M_j)(1 \le j \le n)$

Begin
Compute: $t_j = H_2(T_j \| s_j{}')$;
while $j \le n$ **do**
  $R_{j,1} = A_{j,1}^{-\lambda'_j} \cdot u^{s_{j,\alpha}}$
  $R_{j,2} = A_{j,2}^{-\lambda'_j} \cdot v^{s_{j,\beta}}$
  $R_{j,4} = A_{j,1}^{s_{j,x}} \cdot u^{-s_{j,\gamma_1}}$
  $R_{j,5} = A_{j,2}^{s_{j,x}} \cdot v^{-s_{j,\gamma_1}}$
  Verify:
  $\lambda_j \stackrel{?}{=} H(M_j, A_{j,1}, A_{j,2}, A_{j,3}, R_{j,1}, R_{j,2}, R_{j,3}, R_{j,4}, R_{j,5})$
  j=j+1
end while
Give $\theta_j = \lambda_j / t_j$
Verify:
$e(\prod_{j=1}^{n} (A_{j,3}^{s_{j,x}} \cdot g_1^{-\theta_j} \cdot h^{-s_{\gamma_1} - s\gamma_2})^{\tau_j}, g_2) \cdot$
$e(\prod_{j=1}^{n} (A_{j,3}^{\theta_j} \cdot h^{-s_{j,\alpha} - s_{j,\beta}})^{\tau_j}, w) \stackrel{?}{=} \prod_{j=1}^{n} R_{j,3}^{\tau_j}$
if true **then**
  Accept n messages
else
  Drop n messages
end if
End

5 Security Analysis and Performance Evaluation

In this section, we present the security analysis and performance evaluations of our scheme.

5.1 Security Analysis

Group signature algorithm is not detailed in this section, as it is out of scope this paper. A detailed description of this algorithm can be found in the works of [2], which also proves the anonymity, security and unforgeablity of the group signature algorithm. The correctness and security of the innovating part of our proposed scheme are proved as follows.

Correctness proof. When the verifier received $gpk = (g_1, g_2, h, u, v, w, H_2)$, M, $\sigma = (A_1, A_2, A_3, R_3, \lambda, s_\alpha, s_\beta, s_x, s_{\gamma_1}, s_{\gamma_2}, s_i{}', T_i)$, he can calculate the correct value of R_1, R_2, R_3, R_4, R_5, if T_i is a real validity, then $\lambda \stackrel{?}{=} H(M, A_1, A_2, A_3, R_1, R_2, R_3, R_4, R_5)$ will be verified, and based on λ and other parameters, and R_3 can be calculated, which will be equal to the R_3 in signature.

The correctness proof process is as follows:

$$
\begin{aligned}
& e(A_3, g_2)^{s_x} \cdot e(h, w)^{-s_\alpha - s_\beta} \cdot e(h, g_2)^{-s_{\gamma_1} - s_{\gamma_2}} \cdot \\
& (e(A_3, w)^{1/t_i} / e(g_1, g_2))^{\lambda} \\
=& e(A_3, g_2)^{r_x + \lambda' x} \cdot e(h, w)^{-r_\alpha - \lambda'\alpha - r_\beta - \lambda'\beta} \cdot \\
& e(h, g_2)^{-r_{\gamma_1} - \lambda'_{\gamma_1} - r_{\gamma_2} - \lambda'_{\gamma_2}} \cdot e(A_3, w)^{\lambda / t_i} \cdot e(g_1, g_2)^{-\lambda} \\
=& e(A_3, g_2)^{\lambda' x} \cdot e(h, w)^{-\lambda'\alpha - \lambda'\beta} \cdot e(h, g_2)^{-\lambda'_{\gamma_1} - \lambda'_{\gamma_2}} \cdot \\
& e(A_3, w)^{\lambda'} \cdot e(g_1, g_2)^{-\lambda} \cdot e(A_3, g_2)^{r_x} \cdot \\
& e(h, w)^{-r_\alpha - r_\beta} \cdot e(h, g_2)^{-r_{\gamma_1} - r_{\gamma_2}} \\
=& e(A_3{}^{\lambda'}, w g_2{}^{x}) \cdot e(h^{-\lambda'\alpha - \lambda'\beta}, w g_2{}^{x}) \cdot e(g_1, g_2)^{-\lambda} \cdot \\
& e(A_3, g_2)^{r_x} \cdot e(h, w)^{-r_\alpha - r_\beta} \cdot e(h, g_2)^{-r_{\gamma_1} - r_{\gamma_2}} \\
=& e(f_i{}', w g_2{}^{x})^{\lambda'} \cdot e(g_1, g_2)^{-\lambda} \cdot e(A_3, g_2)^{r_x} \cdot \\
& e(h, w)^{-r_\alpha - r_\beta} \cdot e(h, g_2)^{-r_{\gamma_1} - r_{\gamma_2}} \\
=& e(g_1, g_2)^{\lambda} \cdot e(g_1, g_2)^{-\lambda} \cdot e(A_3, g_2)^{r_x} \cdot \\
& e(h, w)^{-r_\alpha - r_\beta} \cdot e(h, g_2)^{-r_{\gamma_1} - r_{\gamma_2}} \\
=& e(A_3, g_2)^{r_x} \cdot e(h, w)^{-r_\alpha - r_\beta} \cdot e(h, g_2)^{-r_{\gamma_1} - r_{\gamma_2}} \\
=& R_3
\end{aligned}
$$

$$
\begin{aligned}
R_1 =& A_1^{-\lambda'} \cdot u^{s_\alpha} = u^{-\lambda'\alpha} \cdot u^{r_\alpha + \lambda'\alpha} = u^{r_\alpha} \\
R_2 =& A_1^{-\lambda'} \cdot v^{s_\beta} = v^{-\lambda'\beta} \cdot v^{r_\beta + \lambda'\beta} = v^{r_\beta} \\
R_4 =& A_1{}^{s_x} \cdot u^{-s_{\gamma_1}} = (u^{\alpha})^{r_x + \lambda' x} \cdot u^{-r_{\gamma_1} - \lambda'\alpha x} \\
=& A_1{}^{r_x} \cdot u^{-r_{\gamma_1}} \\
R_5 =& A_2{}^{s_x} \cdot v^{-s_{\gamma_2}} = (v^{\beta})^{r_x + \lambda' x} \cdot v^{-r_{\gamma_2} - \lambda'\beta x} \\
=& A_2{}^{r_x} \cdot v^{-r_{\gamma_2}}
\end{aligned}
$$

In a similar way, the batch verification process can also be validated.

Security proof. When a false user attempts to use an expired membership, he must forge a false validity T' in advance. As the Hash Function is collision resistant, it is probably impossible that the false T' can be an equivalent to the true T. During the signature verification, when someone sends his M, σ and T' to the verifier, the verifier initially checks T'. If this is not valid, the signature verification process cannot be progresses any further, otherwise, the verification process can be carried out as follows:

1) $t'_i = H_2(T'_i \| s_i{}')$
2) Verify the equation:

$$
\begin{aligned}
& e(A_3, g_2)^{s_x} \cdot e(h, w)^{-s_\alpha - s_\beta} \cdot e(h, g_2)^{-s_{\gamma_1} - s_{\gamma_2}} \cdot \\
& (e(A_3, w)^{1/t_i} / e(g_1, g_2))^{\lambda} \stackrel{?}{=} R_3
\end{aligned}
$$

If t_i is not equal to t'_i, $e(f' \cdot w g_2^{x})^{1/t_i} = e(g_1, g_2)$ will be an impossible equation, thus the equation could not be verified and the verification process will be

terminated here. And so the false validity cannot regain the membership and the vehicle needs to reapply for it. In this way, the forward and backward secure revocation is achieved in VANETs. It means that the false vehicle cannot access the services after revocation, and other vehicles cannot access the services as an impostor either. In a similar way, the batch verification process of the Security proof can be validated.

5.2 Performance Evaluation

In this section, firstly, we define the time complexity of the cryptographic operations required between our scheme and other existing schemes. Let m denotes the number of group member, N_{crl} denotes the number of CRL items, T_{mul} denotes the time to compute one point multiplication, T_{mac} denotes the time of one message authentication code operation, T_{par} denotes the time to perform one pairing operation, T_{exp} denotes the time to compute one exponentiation. We consider the time of the four important operations above but neglect the time of the other operations such as additive and one-way hash function in this evaluation. Here, we adopt the experiments in paper [6], which observes processing time [9], where G_1, G_2 is by 161 bits, G_T is by 960 bits and elements in Z_p is by 160 bits, and running on a machine with 1G RAM and a single core CPU with a frequency of 3.0 Hz.

Verification Delay. Our scheme does not consider CRL checking, as it supports batch verification process simultaneously, thereby the checking cost (both the time of checking one signature and n signature) is decreased significantly compared to CRSB and SPRING. Although the verification delay of our scheme consumes more time than VAST, VAST does not consider both anonymity and traceability. In this way, our scheme is superior to VAST. Table 4 displays the combination of the dominant operations of the four signature schemes in terms of authenticating a single signature and n signatures, respectively. It can be observed from Figure 5, the verification delay of other existing schemes (CRSB,SPRING) significantly varies with an increasing number of messages.

Batch Verification. In general, frequent communication is evident between the vehicles and RSUs, and also between two vehicles in VANETs. Obviously, VANETs deserves shorter verification delays in order to achieve effective communication. Batch verification of our scheme can significantly improve the signature verification efficiency. Before optimization, the verification time of a single message is $12T_{exp}+5T_{par}$. Also the original scheme cannot support batch verification, where the verification time of n pieces of message is $12nT_{exp}+5nT_{par}$. After optimization, our scheme supports batch verification, with a batch verification time of $13nT_{exp}+2T_{par}$. Time to perform one pairing operation is much more

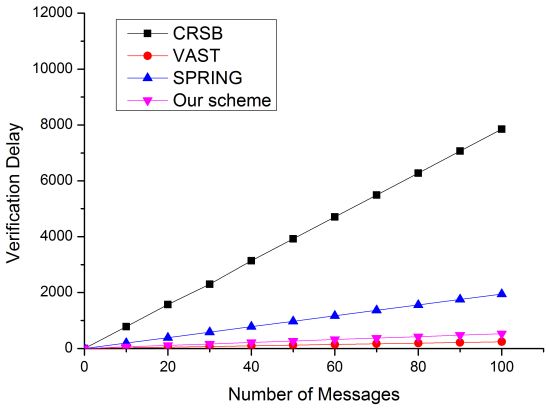

Figure 5: Verification delay versus traffic density

than the time to compute one exponentiation, thus improving the efficiency. Figure 6 depicts the increase in the signature verification delay with the increasing number of messages, between single verification and batch verification. The results show that the efficiency of batch verification is superior to single verification in VANETs.

Transmission Overhead. Communication overheads incurred in the authentication process of a single message is caused by the attached certificate and signature. CRSB verification is based on a ring structure along with a group public key for verifying messages, and so this process does not require the attachment of certificates. The signature length of CRSB is 147 bytes. Communication overhead of VAST includes 63 bytes certificate, 20 bytes message authentication code, 42 bytes signature, 16 bytes symmetric key and 4 bytes of index ID. So the total length of this signature is 63+20+42+16=4=149 bytes. Communication overhead of SPRING includes 121 bytes Short-time certificate, 26 bytes Anonymous key, 40 bytes signature, 2 bytes of Group ID, and so the total length of the signature is 121+26+40+2=189 bytes. Without batch verification in our scheme, the scheme signature consists of 3 elements of G and 8 elements of Z_p, so its byte-length is 3*(161/8)+8*(160/8)=220 bytes, along with the 4 bytes Timestamp, 2 bytes of Message ID. The total length of the signature of Scheme 1 is 220+4+2=226 bytes. There is no significant difference between the length of our Scheme and the length of other existing schemes. When batch verification is included in our scheme, the total signature length is 226+(960/8)=346 bytes because of the additional elements of G_T. The additional signature length overheads incurred in our scheme are acceptable, even though the single signature length of our scheme is greater than that of the other existing schemes. This is because of the higher storage requirements and communication

overheads caused by CRL or PKC in other existing schemes.

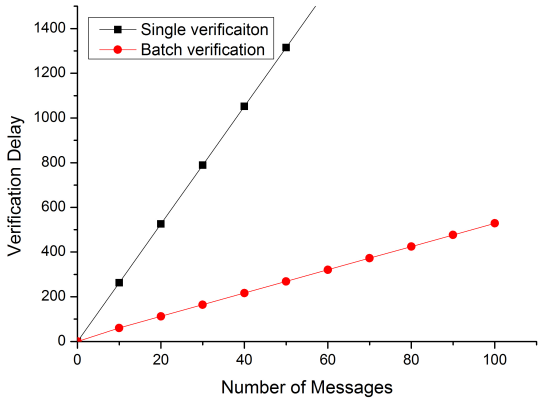

Figure 6: Single verification versus batch verification

Table 4: Comparisons of the speed of four signature schemes

Method	Verify a single signature	Verify n signatures
CRSB [16]	$2T_{par} + 3T_{exp} + mT_{mul} + 9N_{crl}$	$2nT_{par} + 3nT_{exp} + nmT_{mul} + 9N_{crl}n$
VAST [14]	$4T_{mul} + 2T_{mac}$	$4nT_{mul} + 2nT_{mac}$
SPRING [13]	$11T_{mul} + 3T_{par}$	$11nT_{mul} + 3nT_{par}$
Our Scheme	$12T_{exp} + 5T_{par}$	$13nT_{exp} + 2T_{par}$

Average Delay. We use the average delay (AD) to reflect the efficiency. The VAST scheme is neglected in this evaluation due to comparable incompatibility, as it is not supporting privacy protection, the scheme is not comparable with our scheme. A critical comparison is attempted in terms of average delay between our scheme,and CSRB and SPRING, simulated in MATLAB. The signature length of our scheme, CSRB and SPRING are 346 bytes, 147 bytes and 189 bytes respectively. The formulas used in this evaluation are listed as follows:

$$AD_{msg} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(T_s + T_t + \alpha T_C + (1-\beta)T_v) + \beta T_b}{NM}$$

$$\alpha = \begin{cases} 0 & \text{the scheme does not need to check the CRL} \\ 1 & \text{the scheme needs to check the CRL} \end{cases}$$

$$\beta = \begin{cases} 0 & \text{the scheme cannot support batch verification} \\ 1 & \text{the scheme can support batch verification} \end{cases}$$

where AD_{msg} represents the average delay, N represents the total number of vehicles, M is the number of messages sent by a vehicle, T_s is the signature time for a message, T_t is the transmission time for a message, T_C is the CRL checking time for a message, T_v is the verification time for a message, and T_b is the batch verification time for all the messages. As shown in Fig.7, the average delay of our scheme is 32% lesser compared to SPRING, and 40% lesser compared to CSRB respectively. This is because our scheme supports batch verification and also eliminates the need for CRL checks.

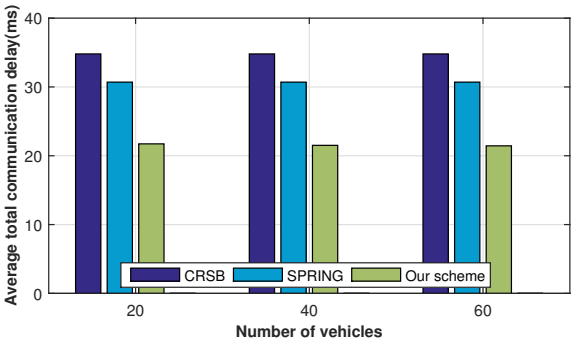

Figure 7: Average delay

6 Conclusion

In this paper, we introduce a new scheme (ECPB) based on group signature for privacy-preserving in VANETs. In our scheme, the validity of membership is required when a vehicle applies for group membership and the validity is used to check whether the requesting vehicle is genuine or not, This validation process can deployed as a substitute for CRL checks. Also, our proposed scheme supports batch authentication of the messages. The security analysis and experimental results show that ECPB delivers the higher efficiency verification requirements of VANETs, and also satisfies the Privacy-preserving Communication for VANETs.

Acknowledgments

The work was supported by the National Natural Science Foundation of China (No. 61173188, No. 61173187), the Research Fund for the Doctoral Program of Higher Education (No. 20133401110004), the Science and technology project of Anhui Province (No. 1401b042015), the Educational Commission of Anhui Province, China (No. KJ2013A017).

References

[1] D. Boneh, X. Boyen, H. Shacham, "Short group signatures," in *proceedings of CRYPTO'04*, pp. 41–55, 2004.

[2] A. L. Ferrara, M. Green, S. Hohenberger, "Practical short signature batch verification," in *Proceedings of*

Topics in Cryptology (CT-RSA'09), LNCS 5473, pp. 309–324, Springer, 2009.

[3] M. Gerlach, "VaneSe-An approach to VANET security," in *Proceedings of the Vehicle-to-Vehicle Communications (V2VCOM'05)*, 2005.

[4] J. Guo, J. P. Baugh, S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," *2007 Mobile Networking for Vehicular Environments*, pp. 103–108, Anchorage, AK, May 2007.

[5] Y. Hao, Y. Cheng, C. Zhou, et al., "A distributed key management framework with cooperative message authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp.616–629, 2011.

[6] S. J. Horng, S. F. Tzeng, Y. Pan, et al., "B-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

[7] J. Li, H. Lu, M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2014.

[8] R. Lu, X. Lin, X. Liang, et al., "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13 no. 1, pp. 127–139, 2012.

[9] B. Lynn, *The Pairing-Based Cryptography Library*, 2013. (`http://crypto.stanford.edu/pbc/`)

[10] M. S. I. Mamun, A. Miyaji, "Secure VANET applications with a refined group signature," in *Twelfth Annual Conference on Privacy, Security and Trust (PST'14)*, pp.199–206, 2014.

[11] M. Mikki, Y. M. Mansour, "Privacy preserving secure communication protocol for vehicular Ad hoc-networks," in *Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 189–195, 2013.

[12] P. Papadimitratos, G. Calandriello, J. P. Hubaux, "Impact of vehicular communications security on transportation safety," in *IEEE INFOCOM Workshops*, pp. 1–6, 2008.

[13] L. Rongxing, L. Xiaodong, S. Xuemin, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proceedings of IEEE INFOCOM'10*, pp. 1–9, 2010.

[14] A. Studer, F. Bai, B. Bellur, et al., "Flexible, extensible, and efficient VANET authentication," *Communications and Networks*, vol. 11, no. 6, pp. 574–588, 2009.

[15] A. Wasef, X. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," in *Proceedings of IEEE ICC'10*, pp. 1–5, Cape Town, South Africa, May 2010.

[16] S. Zeng, Y. Huang, X. Liu, "Privacy-preserving Communication for VANETs with conditionally anonymous ring signature," *International Journal of Network Security*, vol. 17, no. 2, pp. 135–141, Mar. 2015.

[17] C. Zhang, R. Lu, X. Lin, et al., "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of IEEE INFOCOM*, pp. 246–250, Phoenix, AZ, USA, Apr. 2008.

[18] L. Zhang, Q. Wu, A. Solanas, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[19] X. Zhu, S. Jiang, L. Wang, et al., "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, Feb. 2014.

Yimin Wang is a PhD Candidate at the the School of Computer Science and Technology, Anhui University, China. His research interests include security and privacy for wireless networks, cloud computing, big data, etc..

Hong Zhong received her B. S. degree in applied mathematics in Anhui University, China, in 1986, and the Ph.D degree in computer science and technology from University of Science and Technology of China (USTC), China, in 2005. Now she is a professor and Phd Advisor of Anhui University. Her research interests include security protocols and wireless sensor networks.

Yan Xu is reading for a Ph.D in School of Computer Science and Technology at University of Science and Technology of China. Her research interests include information security, cryptography.

Jie Cui is currently an Associate Professor in the School of Computer Science and Technology, Anhui University. He received his PhD degree from University of Science and Technology of China in 2012. He has published 20 papers. His research interests include the design and analysis of symmetric ciphers.