Hindawi
Security and Communication Networks
Volume 2023, Article ID 8676929, 12 pages
https://doi.org/10.1155/2023/8676929

Research Article

A Privacy-Preserving Authentication Scheme for VANETs with Exculpability

Shangle Li, Ruili Yang, and Jiageng Chen

School of Computer Science, Central China Normal University, Wuhan 430079, China

Correspondence should be addressed to Jiageng Chen; chinkako@gmail.com

Received 21 August 2022; Revised 19 December 2022; Accepted 3 January 2023; Published 7 February 2023

Academic Editor: Vijayakumar Pandi

Message authentication and conditional privacy preservation are two critical security issues in VANETs (vehicular ad hoc networks). To achieve the corresponding security goals, many security technologies have been proposed so far. Identity-based pseudonyms and group signature-based schemes are two of the main technologies in recently published literature. However, the key escrow is difficult to achieve and pseudonym identities may reveal the physical location of the vehicle in the identity-based scheme. The global manager TA of VANETs knows the full keys given to the vehicles and can forge signatures under the vehicle's key. Therefore, the exculpability cannot be satisfied in the group signature scheme. To address these security issues, a privacy-preserving authentication scheme for VANETs with exculpability is proposed in this paper, which applies double key approach to realize the trusted communication between vehicle and road side units and TA by combining the advantage of group-based methods and identity-based methods. Security analysis shows that the security of our scheme can resist stronger attacks than previous schemes.

1. Introduction

The application of vehicular ad hoc networks (VANETs) has become a hot topic in the smart city [1]. A typical VANETs system consists of three parts: TA (trusted authority), RSUs (road-side units), and vehicles. The global manager TA of VANETs controls the system to ensure normal operation. The RSUs are distributed on the road and forward messages between vehicles and TA. The vehicles are equipped with OBU (on-board units).

There are two types of communication in VANETs: V2V communication and V2I communication. The V2V communication has taken place between vehicles. The vehicle broadcasts messages to nearby vehicles. The communication between vehicles and RSUs is called V2I communication. However, according to DSRC protocol [2], various attacks exist in the wireless communication environment [1, 3]. Thus, it is very important to protect the privacy of the vehicles.

To prevent message spoofing, all messages are signed by secret keys generated by a tamper-proof device (TPD) [4, 5], but the TPD is very expensive. Even worse, a signing key can be revoked if the TPD of a car is compromised. Nevertheless, many previous identity-based signature (IBS) schemes [5] for VANETs rely on the TPD to store the signing key.

In many IBS schemes, the real identity of the vehicle is coded as the pseudo-ID (PID) to protect the privacy of the vehicle. But the real identity of the vehicle might be recovered from the PID [6]. In addition, attackers may track the PID of the vehicle directly without recovering the real identity of the vehicle. Even worse, many schemes do not update the key for a long time, and attackers locate the vehicle by continuously tracking the single public key or PID of a vehicle without decrypting the message.

In many previous short group signature schemes [6, 7] for VANETs, the secret key of the vehicle used to sign messages cannot be hidden from the group managers, say TA, which has no exculpability property for the vehicle. The exculpability [8] asks that the key issuer cannot know the full secret key given to the vehicle and so cannot produce signatures under the vehicle's key [9].

The BV-CLRS scheme [10] proposed by Bouakkaza and Semchedineb is based on traceable certificate-less ring

signature with exculpability. Exculpability means that no member in the group can forge the signatures of other members, even the administrator. Then, the computation and communication overhead are optimized in the CLA-TRS scheme [11]. In the earlier short group signature scheme [9], Dan Boneh proposed the idea of applying strong exculpability in VANETs.

Due to the special topology of VANETs that vehicles are moving at high speed, and the network connection is frequently changing, vehicles broadcast message approximately every 100 milliseconds [10, 12]. Therefore, the length of signature should be under 250 bytes [9] for the efficiency purpose.

In this paper, we propose and develop a privacy-preserving authentication scheme for VANETs. In our scheme, TA generates a partial key for the vehicle, as the key generation algorithm of short group signature [9] does using the vehicle's public key. Therefore, the full signing key of the vehicle is no longer shared with TA so that the vehicle cannot deny the signature signed by itself with its signing key. The vehicle signs message with full signing key and broadcasts the signature to vehicles and RSUs nearby. The length of the signature which is signed by short group signature algorithm is not more than 250 bytes. More precisely, the PID of a vehicle is not included in the signature as the IBS scheme [5] did. The attacker cannot locate the vehicle by tracking the PID, and the PID is hidden in a private parameter saved by the TA. The RSU which is semitrusted forwards messages between TA and vehicles.

In summary, this paper has four-fold main contributions:

(i) We propose a privacy-preserving authentication scheme for VANETs with exculpability. The advantage of our scheme is that the signature of the vehicle has strong exculpability. No vehicle can deny the signature signed by itself, and the TA cannot sign in place of the vehicle.

(ii) In our scheme, the vehicle has the full signing key and will update keys online by itself easily. The vehicle can automatically update the key online periodically without relying on the TA.

(iii) The signature of messages does not contain any information about the real identity of the vehicle, and the attackers cannot locate the vehicle by tracking the PID of the vehicle. No one can track the vehicle except the TA.

(iv) We analyze the security of the proposed scheme and compare the security strength of the related schemes which shows our advantage. Finally, The performance of each scheme is analyzed and compared theoretically and practically.

The remainder of this paper is organized as follows. In Section 2, we briefly reviewed the related works. The preparatory knowledge related to this paper is shown in Section 3. In Section 4, we presented the authentication scheme for VANETs and analyzed the security in Section 5. In Section 6, we analyzed the performance of the scheme and simulate the protocol. We summarized this paper in the last Section.

2. Related Work

In wireless communication of VANETs, there exists various kinds of attacks [3]. Message authentication and privacy preservation are two critical security issues in VANETs.

Identity-based and group signature-based are two of the main technologies to realize the security requirements for VANETs. An identity-based conditional privacy-preserving authentication (CPPA) scheme was proposed by He et al. [5]. In CPPA scheme, the TA presets secret keys for vehicles and publishes the corresponding public keys. The tamper-proof device (TPD) of the vehicle generates the pseudonymous identity (PID) and session key for the vehicle. However, the PID of the vehicle is exposed to the wireless environment and may be tracked. In group signature-based schemes [6, 7, 13], the group manager issues the private key to the vehicle, and the vehicle signs the message with the private key. So the vehicles would deny the signature signed by themselves and strong exculpability cannot be satisfied.

Key distribution and update for the vehicles are not efficient in some ID-based or group signature-based schemes. In CPPA scheme [5], the TA presets the secret key for the vehicles and the key cannot be updated online. Solutions [13, 14] tried to solve the problem of key allocation but the key update is not very efficient. The common feature is that the key of the vehicle fully depends on the administrator distribution.

Bilinear-pairing is a common cryptography primitive used for message authentication in VANETs, but its computational complexity is relatively high. To encoded the real identity of a vehicle, two different pseudo-IDs are generated for the same session in the scheme proposed by Zhang et al. [15], but the scheme cannot defend the denial-of-service (DoS) attack. The implementation of the ID-based CPPA scheme [5] removes the bilinear-pairing, but the PID of the vehicle is exposed.

In ID-based scheme, the TPD where the secret key of the vehicle is memorized is always used as a necessary module of the vehicle to protect the security of the secret key [4, 5, 15], but the device is not cheap. If the TPD is attacked, such as a side-channel attack, the forward security of the protocol will be threatened.

Due to the special topology of VANETs, the protocols require minimizing the overhead of the message signature broadcasted by the vehicle. The pseudo-ID of the vehicle is used as a public key in reducing the size of the signature in an ID-based scheme [5]. Some group signature-based schemes [14] use the short group signatures of Dan et al. [9] to minimize the signature size.

The BV-CLRS scheme [10] based on ring signature compresses the length of the signature to a certain extent. The scheme emphasizes the security of exculpability of the vehicle. Subsequently, Samra and Fouzi [11] further compressed the computation and communication overhead based on ring signatures.

Batch verification technology is used to improve the efficiency of message verification in many schemes [5, 10, 11]. But if the batch verification of messages fails, it may cause more delay. So some group testing methods are proposed to detect the negative samples of the signatures.

An ideal protocol for VANETs should preserve the privacy of the vehicle, prevent the tracking of the vehicle, authenticate the message of the sender, and so on. Unfortunately, the schemes discussed above lack one or more of the required features, which motivates our proposal.

3. Preliminaries

3.1. Bilinear Pairing. We first review the definition of bilinear maps [9].

(i) G_0 and G_1 are two cyclic groups of prime order p;

(ii) g_0 and g_1 are two generators of G_0 and G_1, respectively;

(iii) φ is a computable isomorphism from G_1 to G_0, as $g_0 = \varphi(g_1)$;

(iv) e is a computable map $e: G_0 \times G_1 \longrightarrow G_T$ and satisfies the following properties:

(i) Bilinearity: for all $u \in G_0$, $v \in G_1$, and $\alpha, \beta \in \mathbb{Z}$, such that $e(u^\alpha, v^\beta) = e(u, v)^{\alpha\beta}$.

(ii) Nondegeneracy: $e(g_0, g_1) \neq 1$.

In this paper, we consider $G_0 = G_1 = G$. To achieve the same level of security as a standard 1024-bit RSA signature [9], we used the fact that G can be of size 22-byte whose elements are 171-bit string, and the DL problem in G is as hard as the one in $\mathbb{Z}_q^*$, where q is 1020 bits in length. For convenience, we assumed that isomorphism φ exists and is computable efficiently.

3.2. A ZK Protocol for SDH. We follow the ZKPK protocol [9] and JOIN protocol [8] to present the underlying building block for our scheme.

3.2.1. Key Generation. Given the public values $(g_0, g_1, u, v \in G)$ and selected $(\alpha, \beta) \in \mathbb{Z}_p$ such that $u^\alpha = v^\beta = h$, where $h \in G/\{1_G\}$. The pair $(\alpha, \beta) \in \mathbb{Z}_p$ is the tracing key.

Select private key $\gamma \in \mathbb{Z}_p$ and set $\mu = g_1^\gamma$. Select private keys $x, y \in \mathbb{Z}_p$, generate pair (A, x, y) for each user where $A \in G$, such that $A^{\gamma+x} \cdot h^y = g_0$.

The pair (A, x, y) satisfies $e(A, \mu g_1^x) \cdot e(h, g_1^y) = e(g_0, g_1)$, and the pair (x, y) is a private key with two keys. Moreover, the partial key x is generated from a $(q+2)$-tuple $(g_0, g_1, g_1^\gamma, g_1^{\gamma^2}, \ldots, g_1^{\gamma^q})$ with private key γ under the SDH assumption, and output a pair $((g_0/h^y)^{1/(\gamma+x)}, x)$.

3.2.2. Sign. The user signs message m with private keys (x, y) and outputs signature σ.

$$\sigma \longleftarrow \left(T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_y, s_{\delta_1}, s_{\delta_2}\right). \tag{1}$$

The private key of user is the exponents (x, y). The user randomly chooses $a, b \in \mathbb{Z}_p$ and encrypts the message $m \in G$, and output $(T_1, T_2, T_3) = (u^a, v^b, m \cdot h^{a+b})$ of signature σ. The Linear encryption (T_1, T_2, T_3) of A under public key (u, v, h), and corresponds tracing key (α, β). The message m can be derived from (T_1, T_2, T_3) by computing $T_3/(T_1^a \cdot T_2^b)$.

$$\begin{aligned}
&T_1 \longleftarrow u^a, T_2 \longleftarrow v^b, T_3 \longleftarrow A h^{a+b},\\
&\delta_1 \longleftarrow xa, \delta_2 \longleftarrow xb,\\
&R_1 \longleftarrow u^{r_a}, R_2 \longleftarrow v^{r_b},\\
&R_3 \longleftarrow e(T_3, g_1)^{r_x} \cdot e(h, \mu)^{-r_a - r_b} \cdot e(h, g_1)^{-r_{\delta_1} - r_{\delta_2}} \cdot e(h, g_1)^{r_y},\\
&R_4 \longleftarrow T_1^{r_x} \cdot u^{-r_{\delta_1}}, R_5 \longleftarrow T_2^{r_x} \cdot v^{-r_{\delta_2}},\\
&c \longleftarrow H(m, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5),\\
&s_a = r_a + ca, s_b = r_b + cb,\\
&s_x = r_x + cx, s_y = r_y + cy,\\
&s_{\delta_1} = r_{\delta_1} + c\delta_1, s_{\delta_2} = r_{\delta_2} + c\delta_2,
\end{aligned} \tag{2}$$

where $r_a, r_b, r_x, r_y, r_{\delta_1}, r_{\delta_2} \in \mathbb{Z}_p$.

The advantage of an efficient algorithm $\mathcal{A}$ in deciding the DL (decision linear) problem [9] in G is shown in the following equation:

$$\mathrm{Adv}_{\mathcal{A}}^{dl} := = \left| \begin{array}{l} \Pr\left[\mathcal{A}\left(u, v, h, u^a, v^b, h^{a+b}\right) = \text{true: } u, v, h \in_R G, a, b \in_R \mathbb{Z}_p\right] \\ -\Pr\left[\mathcal{A}\left(u, v, h, u^a, v^b, \eta\right) = \text{true: } u, v, \eta \in_R G, a, b \in_R \mathbb{Z}_p\right] \end{array} \right|. \tag{3}$$

Definition 1. The linear encryption (LE) scheme is semantically secure against a chosen-plaintext attack, assuming decision linear assumption holds in G if no t-time algorithm has advantage at least ε in solving the decision linear problem in G.

Theorem 1. *The ZK protocol is CPA-fully-anonymous if linear encryption (LE) scheme is semantically secure on G.*

Theorem 2. *Assuming decision linear assumption holds in G, then the ZK protocol is fully-traceable.*

The ZK protocol is fully-anonymous and fully-traceable under the Theorems 1 and 2.

(i) Fully-anonymous: the user's private key is only known to herself, and no one, including the group manager, knows about it.

(ii) Fully-traceable: the group manager can recover the user identity information by using the tracing key.

Definition 2. Exculpability is informally defined as not a member of the group and not even the group manager given the tracing key can produce signatures on behalf of other users [9, 16].

The ZK protocol has the exculpability property. The signing keys (x, y) are generated by the manager and the user. But only the user knows the full keys (x, y), the manager only knows the partial key x which is an exponent of the SDH tuple.

4. The System Model

In this section, we propose our privacy-preserving authentication scheme for VATENs. We define the notations used as shown in Table 1.

4.1. Architecture. In our scheme, the architecture (as illustrated in Figure 1) consists of three entities: fully trusted TA, RSU, and vehicles.

TA interacts with RSUs directly. But the interaction between the TA and vehicles is through RSUs.

The RSU periodically broadcasts public values to vehicles.

V2V communication: the vehicle broadcasts message to vehicles nearby. V2I communication: the vehicle broadcasts message to RSU nearby.

4.1.1. TA. The TA (trusted authority) is the global manager of the system and is fully trusted. The TA initiates and generates system parameters. The RSUs and vehicles will register at TA and are given certificates and public keys. The TA interacts with RSUs directly, and the interaction with vehicles through RSUs. The TA is also responsible for the revocation of malicious vehicles.

4.1.2. RSU. The RSUs (road-side units) are roadside infrastructures distributed evenly on both sides of the road and considered untrusted which are vulnerable to geographic attacks. RSUs interact directly with the TA and are in charge of monitoring vehicles for suspicious activity and reporting back to it and forward messages between the TA and vehicles. The RSU periodically broadcasts public values to vehicles in its radiation region. The communication between RSUs and vehicles is called V2I communication. The TA will broadcast revocation list to RSUs to revoke the malicious vehicle from the system.

4.1.3. Vehicle. The vehicles are instances of on-board units (OBUs) moving on the road. The vehicles will broadcast useful messages (speed, traffic accident, etc.) to nearby vehicles and RSUs. The communication between vehicle to vehicles is called V2V communication. The vehicles are vulnerable entities in the system. Therefore, the privacy of vehicles must be protected.

4.2. Security Requirements. The survey of Sheikh et al. [3] lists various attacks in VANETs. According to the specifications of DSRC protocol [2] and VANET security services in traffic management system [1], various security requirements should be considered.

(i) Authentication: To ensure the security of the system, the identity of vehicles must be authenticated. The message receiver can detect invalid messages from suspicious vehicles. The TA is able to reveal malicious vehicles, and RSUs can execute the order from the TA to remove the bad ones from the group.

(ii) Privacy: The identities and locations of the vehicles are sensitive information for users that may reveal the habits of drivers. The message receivers (say, RSUs and vehicles) should not know the sensitive information. The other parties should not be able to derive private messages from transcripts between V2V communication and V2I communication. TA can extract the privacy information from vehicles.

(iii) Tracing: In order to prevent malicious vehicles from releasing false information to evade responsibility, TA has the right to track vehicles. The TA extracts the vehicle's real identity by deciphering the messages when it is necessary. As for other entities, they have no ability to achieve it.

(iv) Unlikability: RSUs and malicious vehicles cannot link two messages from the same vehicle. For example, RSUs cannot identify if two signatures are from the same vehicle or not.

While achieving the above security properties, our scheme can provide a stronger security requirement, namely, the exculpability property. As introduced by Ateniese and Tsudik [16] and Bellare et al. [17], no member of the group and not even the group manager can produce signatures on behalf of other users. As stronger exculpability requires that even the entity that issues user keys cannot forge signatures on behalf of users [18]. The security requirements listed below are satisfied if the security of exculpability is applied.

(i) The vehicle cannot deny the signature signed by itself, because only the vehicle has a complete private key. The attacker cannot generate a valid signature.

(ii) No one in the group can forge member signatures, including the group administrator, let alone the adversary. The TA or the attacker can ask the private key of the vehicle, but cannot generate a valid signature.

Table 1: The notations of the execution time of cryptography operations.

Notations	Description
G	Two cyclic groups $G_0 = G_1$ of prime order p, denoted as G
g_0, g_1	Two generators of G
u, v, h	Three generators of G
γ	The private key of the TA
α, β	Two integers of $\mathbb{Z}_p^*$
H	A hash function: $\{0,1\}^* \longrightarrow \mathbb{Z}_p$
y_i	The partial private key of vehicle V_i generated by V_i
x_i	The partial private key of vehicle V_i generated by TA
PK_i	The public key of vehicle V_i
sk_i	The full-private key of vehicle V_i
σ	The signature of message M
A_i	The private value of vehicle which is bound to the real identity

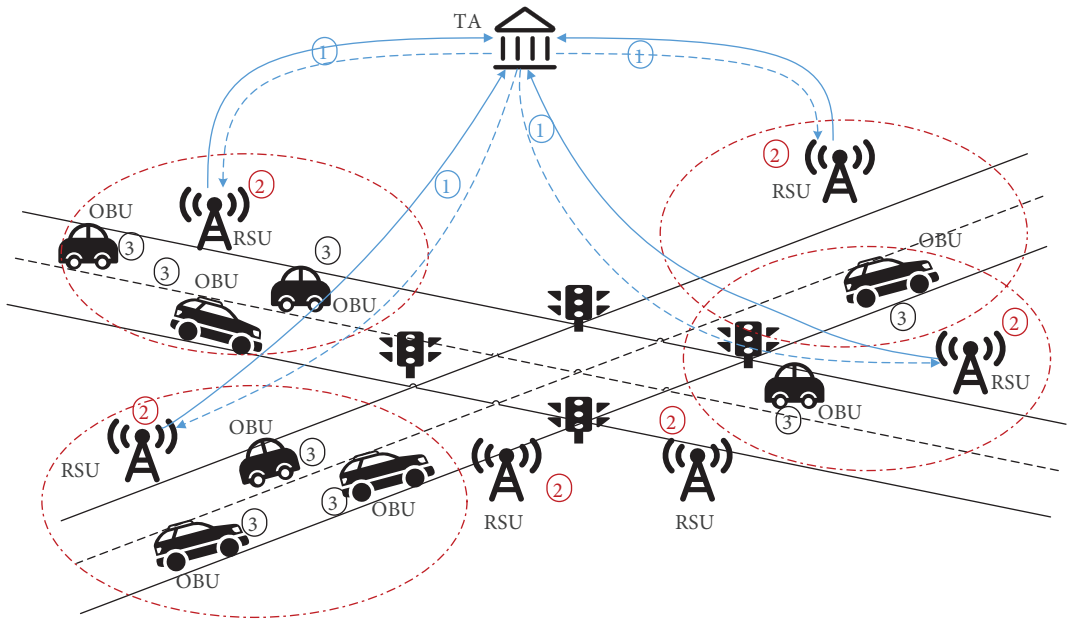

Figure 1: System model.

(iii) The vehicle can periodically update the session key online. Except for the TA, no one can get the sensitive information of the vehicle through the communication transcript. The private key update of the vehicle does not need to rely on TA. During the key update process, the attacker cannot forge the private key of the vehicle.

(iv) Except for the TA, no one can associate the PID and position information of the vehicle to locate the vehicle. The PID of the vehicle will be completely hidden. The attacker can intercept all communication transcript, but cannot analyze the vehicle's action trajectory through the PID.

(v) Even if the RSU is coerced, it will not threaten the privacy and safety of the vehicle. The private key used for signing is generated by the vehicle itself and can be updated at any time. An attacker can hijack the RSU, but the privacy of the vehicle will not be compromised.

4.3. Algorithms. In this paper, the privacy-preserving authentication scheme for VANETs proposed by us include five algorithms: initiation, registration, signing, verification, and update algorithm. The detailed description of the algorithm is as follows:

4.3.1. Initiation. TA selects generators u, v, h and g_0, g_1 from cyclic group G, picks system private key γ and tracing key $\alpha, \beta \in_R \mathbb{Z}_p^*$, computes $\mu = g_1^{\gamma}$, and then employs secure hash function H. TA publishes the public parameters $(g_0, g_1, u, v, \mu, h, H)$.

4.3.2. Registration. The vehicle V_i selects a partial private key y_i, computes $PK_i = h^{y_i}$, and sends PK_i to TA, which generates and sends back a secret key x_i and private value A_i. The V_i gets secret key $sk_i := (x_i, y_i)$ and private value A_i.

4.3.3. Signing. Given public key (g_0, g_1, u, v, μ, h), secret key (x_i, y_i), A_i, and a message M, compute and output a signature

$$\sigma \longleftarrow \left(T_1, T_2, T_3, T_4, c, s_\alpha, s_\beta, s_x, s_y, s_{\delta_1}, s_{\delta_2}\right), \tag{4}$$

where c is a challenger value.

4.3.4. Verification. The receiver verifies the validity of the signature and verifies the revocation of revoked vehicle. Given signature σ and public key (g_0, g_1, u, v, μ, h) to compute $(\widetilde{R}_1, \widetilde{R}_2, \widetilde{R}_3, \widetilde{R}_4, \widetilde{R}_5, \widetilde{R}_6)$, and then check the following relation:

$$c \stackrel{?}{=} H\left(M, T_1, T_2, T_3, T_4, \widetilde{R}_1, \widetilde{R}_2, \widetilde{R}_3, \widetilde{R}_4, \widetilde{R}_5, \widetilde{R}_6\right), \tag{5}$$

where c is a challenge value generated by the signer. If the signature is valid, then verify whether A is encoded in (T_3, T_4) by testing $e(T_3/A, u) \stackrel{?}{=} e(T_4, h)$, where $A \in RL = \{A_1^*, \ldots, A_n^*\}$. If no element A of RL is encoded in (T_3, T_4), the signer of σ has not been revoked.

4.3.5. Tracing. Using the tracing key (α, β) and (T_1, T_2, T_3) which is in the signature σ, the TA can reveal the signer's identity by computing A_i.

4.3.6. Update. Given new public key $\widehat{PK}_i$ to TA, TA returns $(\widehat{A}_i^*, \widehat{x}_i)$, the vehicle updates public key (g_0, g_1, u, v, μ, h) to the new public key $(\widehat{g}_0, \widehat{g}_1, u, v, \widehat{\mu}, h)$, update secret key (x_i, y_i) to $(\widehat{x}_i, \widehat{y}_i)$, and A_i update to $\widehat{A}_i^*$. The TA broadcasts the new public key $(\widehat{g}_0, \widehat{g}_1, u, v, \widehat{\mu}, h)$.

4.4. System Construction. In this subsection, we provide detailed description of the process of our scheme as follows:

4.4.1. System Initialization. In this phase, TA initiates the system. TA picks the private key γ which is selected randomly from $\mathbb{Z}_p^*$, and then computes $\mu = g_1^\gamma$, where g_1 is a generator of multiplicative cyclic group G. TA selects $h \in_R (G/\{1_G\})$ and $\alpha, \beta \in_R \mathbb{Z}_p^*$, and sets $u, v, h \in G$ such that $u^\alpha = v^\beta = h$, where u, v are generators of multiplicative cyclic group G, and (α, β) is a tracing key. TA employs a secure hash function $H: \{0,1\}^* \longrightarrow \mathbb{Z}_p$ which is used as a random oracle in the proof of security. TA publishes the public parameters $(g_0, g_1, u, v, \mu, h, H)$.

4.4.2. The Registration of Vehicles. In this phase, the vehicle registers at TA through secure channel. The vehicle V_i selects $y_i \in_R \mathbb{Z}_p^*$ as a partial private key and computes $PK_i = h^{y_i} \in G$ and sends PK_i to the TA. The TA generates and sends back a SDH tuple (A_i, x_i) by picking $x_i \in_R \mathbb{Z}_p^*$ and setting $A_i \longleftarrow (g_0/PK_i)^{1/(\gamma + x_i)}$, where A_i regards as pseudo-ID of the vehicle V_i. In addition, the value A_i is bound to the real identity of the vehicle V_i, and A_i can be derived by the TA. The secret key of vehicle V_i is $sk_i := (x_i, y_i)$.

The public key PK_i of vehicle is used to register to TA. The private key sk_i consists of two partial keys x_i and y_i. The partial key y_i is generated by the vehicle and updated periodically or deliberately. The partial key x_i is generated by TA under the public key pk_i corresponding to y_i. Both private keys x_i and y_i are used for the signature.

The vehicle V_i will get secret key $sk_i := (x_i, y_i)$ and private value A_i after this phase.

4.4.3. Message Signing. In this phase, the vehicle signs messages before broadcasting them. Given public key (g_0, g_1, u, v, μ, h), secret key (x_i, y_i), A_i, and a message $M \in \{0,1\}^*$, the vehicle computes and outputs a signature σ as follows:

$$\sigma \longleftarrow \left(T_1, T_2, T_3, T_4, c, s_\alpha, s_\beta, s_x, s_y, s_{\delta_1}, s_{\delta_2}\right). \tag{6}$$

(i) Select randomness $a, b \in_R \mathbb{Z}_p$ as session keys and compute $T_1 \longleftarrow u^a, T_2 \longleftarrow v^b, T_3 \longleftarrow A_i h^{a+b}, T_4 \longleftarrow u^{a+b}$ and $\delta_1 \longleftarrow x_i a, \delta_2 \longleftarrow x_i b$.

(ii) Pick random values $r_\alpha, r_\beta, r_x, r_y, r_{\delta_1}, r_{\delta_2} \in_R \mathbb{Z}_p^*$, and then compute $(R_1, R_2, R_3, R_4, R_5, R_6)$ as follows:

$$\begin{aligned} &R_1 \longleftarrow u^{r_\alpha}, R_2 \longleftarrow v^{r_\beta}, \\ &R_3 \longleftarrow e\left(T_3, g_1\right)^{r_x} \cdot e(h, \mu)^{-r_\alpha - r_\beta} \\ &\qquad \cdot e\left(h, g_1\right)^{-r_{\delta_1} - r_{\delta_2}} \cdot e\left(h, g_1\right)^{r_y}, \\ &R_4 \longleftarrow T_1^{r_x} \cdot u^{-r_{\delta_1}}, R_5 \longleftarrow T_2^{r_x} \cdot v^{-r_{\delta_2}}, \\ &R_6 \longleftarrow T_4^{r_x} u^{-r_{\delta_1} - r_{\delta_2}}. \end{aligned} \tag{7}$$

(iii) Compute challenge value as follows:

$$c \longleftarrow H\left(M, T_1, T_2, T_3, T_4, R_1, R_2, R_3, R_4, R_5, R_6\right). \tag{8}$$

(iv) Compute helper values $(s_\alpha, s_\beta, s_x, s_y, s_{\delta_1}, s_{\delta_2})$ as follows:

$$\begin{aligned} &s_\alpha = r_\alpha + ca, s_\beta = r_\beta + cb, \\ &s_x = r_x + cx_i, s_y = r_y + cy_i \\ &s_{\delta_1} = r_{\delta_1} + c\delta_1, s_{\delta_2} = r_{\delta_2} + c\delta_2. \end{aligned} \tag{9}$$

(v) Broadcast signature σ.

Note that, G is of size 22-byte and elements in G are 171-bit strings and p is a 170-bit prime. The signature of our scheme is formed as follows:

$$\left(T_1, T_2, T_3, T_4, c, s_\alpha, s_\beta, s_x, s_y, s_{\delta_1}, s_{\delta_2}\right), \tag{10}$$

where $c, s_\alpha, s_\beta, s_x, s_y, s_{\delta_1}, s_{\delta_2} \in \mathbb{Z}_p$ and $T_1, T_2, T_3, T_4 \in G$. So, the total length of the signature is $171 \times 4 + 170 \times 7 = 1874$ bits = 235 bytes.

4.4.4. Message Verification. In this phase, the receiver verifies the validity of the signature from the vehicles as well as the revocation status of the revoked vehicle.

(i) Signature verification: given signature σ and public key (g_0, g_1, u, v, μ, h) to compute $(\widetilde{R}_1, \widetilde{R}_2, \widetilde{R}_3, \widetilde{R}_4, \widetilde{R}_5, \widetilde{R}_6)$ as follows:

$$\begin{aligned}
&\widetilde{R}_1 \longleftarrow u^{s_\alpha} T_1^{-c}, \widetilde{R}_2 \longleftarrow v^{s_\beta} T_2^{-c}, \widetilde{R}_3 \longleftarrow e(T_3, g_1)^{s_x} \cdot e(h,\mu)^{-s_\alpha - s_\beta} \\
&\quad \cdot e(h, g_1)^{-s_{\delta_1} - s_{\delta_2}} \cdot e(h, g_1)^{s_y} \left(\frac{e(T_3, \mu)}{e(g_0, g_1)}\right)^c, \\
&\widetilde{R}_4 \longleftarrow T_1^{s_x} u^{-s_{\delta_1}}, \widetilde{R}_5 \longleftarrow T_2^{s_x} v^{-s_{\delta_2}}, \\
&\widetilde{R}_6 \longleftarrow T_4^{s_x} u^{-s_{\delta_1} - s_{\delta_2}}.
\end{aligned} \tag{11}$$

The receiver checks the challenge value c by testing as follows:

$$c \stackrel{?}{=} H(M, T_1, T_2, T_3, T_4, \widetilde{R}_1, \widetilde{R}_2, \widetilde{R}_3, \widetilde{R}_4, \widetilde{R}_5, \widetilde{R}_6). \tag{12}$$

The receiver will proceed if the relation holds. Otherwise, she will report the suspicious vehicle to TA.

$$\begin{aligned}
&e(T_3, g_1)^{s_x} \cdot e(h,\mu)^{-s_\alpha - s_\beta} \cdot e(h, g_1)^{-s_{\delta_1} - s_{\delta_2}} \cdot e(h, g_1)^{s_y} \\
&= e(T_3, g_1)^{r_x + cx_i} \cdot e(h,\mu)^{-r_\alpha - ca - r_\beta - cb} \cdot e(h, g_1)^{-r_{\delta_1} - c\delta_1 - r_{\delta_2} - c\delta_2} \cdot e(h, g_1)^{r_y + cy_i} \\
&= e(T_3, g_1^{x_i})^c \cdot e(T_3, g_1)^{r_x} \cdot e\left(h^{-a-b}, \mu\right)^c \cdot e(h,\mu)^{-r_\alpha - r_\beta} \cdot e(h, g_1)^{-r_{\delta_1} - r_{\delta_2}} \cdot e\left(h^{-a-b}, g_1^{x_i}\right)^c \cdot e(h, g_1)^{r_y} \cdot e(h, g_1^{y_i})^c \\
&= e(T_3, g_1^{x_i})^c \cdot e\left(h^{-a-b}, \mu\right)^c \cdot e\left(h^{-a-b}, g_1^{x_i}\right)^c \cdot e(h, g_1^{y_i})^c \cdot R_3 \\
&= e\left(T_3 h^{-a-b}, \mu g_1^{x_i}\right)^c \cdot e(T_3, \mu)^{-c} \cdot e(h, g_1^{y_i})^c \cdot R_3 \\
&= \left(e(A_i, \mu g_1^{x_i}) \cdot e(h, g_1^{y_i}) / e(T_3, \mu)\right)^c \cdot R_3 \\
&= \left(e(g_0, g_1) / e(T_3, \mu)\right)^c \cdot R_3.
\end{aligned} \tag{13}$$

The calculation process of $\widetilde{R}_3$ of the equation (11) is shown in equation (13), where $T_3 = A_i h^{a+b}$ and $A_i \longleftarrow (g_0/(h^{y_i}))^{1/(\gamma + x_i)}$, $\mu = g_1^{\gamma}$, and the expression is valid

$$e(A_i, \mu g_1^{x_i}) \cdot e(h, g_1^{y_i}) = e(g_0, g_1). \tag{14}$$

The calculation process of $\widetilde{R}_6$ of the equation (11) is shown in the following equation:

$$\begin{aligned}
&T_4^{s_x} u^{-s_{\delta_1} - s_{\delta_2}} \\
&= u^{(a+b)(r_x + cx_i)} u^{-\left(r_{\delta_1} + c\delta_1\right) - \left(r_{\delta_2} + c\delta_2\right)}, \\
&= u^{(a+b)(r_x + cx_i)} u^{-\left(r_{\delta_1} + cax_i\right) - \left(r_{\delta_2} + cbx_i\right)}, \\
&= u^{(a+b)r_x} u^{-r_{\delta_1} - r_{\delta_2}}, \\
&= R_6.
\end{aligned} \tag{15}$$

The verification process of $(\widetilde{R}_1, \widetilde{R}_2, \widetilde{R}_4, \widetilde{R}_5)$ is similar to $\widetilde{R}_6$ and we omit it here.

(ii) Revocation verification: We refer to the VLR (verifier-local revocation) mechanism proposed by Boneh and Shacham [19]. Suppose revocation list (RL) contains the private value of all revoked vehicles. More precisely,

$$RL = \{A_1^*, \ldots, A_n^*,\}. \tag{16}$$

where A_i^* is traced by TA. For each element $A \in RL$, check whether A is encoded in (T_3, T_4) by testing if

$$e(T_3/A, u) \stackrel{?}{=} e(T_4, h). \tag{17}$$

If no element A of RL is encoded in (T_3, T_4), then the signer has not been revoked. Otherwise, some $A_i^* = A$ indicates that the vehicle V_i has been revoked.

The signature σ is valid if it passes both verifications.

4.4.5. Vehicles Tracing. In this phase, TA has the ability to trace the signer of the messages. Using the tracing key and values (T_1, T_2, T_3) in the signature σ, TA can reveal the signer's identity which is related to A_i by computing $A_i \longleftarrow (T_3/(T_1^{\alpha} \cdot T_2^{\beta}))$. To hide the identity of the vehicle, the parameter A_i related to the real identity of a vehicle is a private value saved by TA.

Since the TA holds tracing key (α, β), $u^{\alpha} = v^{\beta} = h$, and $T_1 \longleftarrow u^a, T_2 \longleftarrow v^b, T_3 \longleftarrow A_i h^{a+b}$, then

$$\begin{aligned}
\frac{T_3}{T_1^{\alpha} \cdot T_2^{\beta}} &= \frac{A_i h^{a+b}}{(u^a)^{\alpha} \cdot \left(v^b\right)^{\beta}}, \\
&= \frac{A_i h^{a+b}}{h^a \cdot h^b}, \\
&= A_i.
\end{aligned} \tag{18}$$

The A_i is derived from (T_1, T_2, T_3) with tracing key (α, β).

4.4.6. Key Update. In this phase, the vehicles can update their secret keys online by themselves. For example, the vehicle V_i sends the new public key $\widehat{PK}_i$ through some authenticated channel, where $\widehat{PK}_i = h^{\widehat{y}_i}$. TA will compute

new SDH pair $(\widehat{A}_i^*, \widehat{x}_i)$, and then send back $(\widehat{A}_i^*, \widehat{x}_i)$, where $\widehat{A}_i^* = (g_1/\widehat{PK}_i)^{(1/(\gamma+x_i))}$. The vehicle will update its public key and secret key as follows.

Note that $g_0 = \varphi(g_1)$ and $A_i = \varphi(\widehat{A}_i^*)$. Given public key $\widehat{PK}_i$, TA will use private key γ to compute the $\widehat{A}_i^*$ and send back $(\widehat{A}_i, \widehat{x}_i)$. The vehicle with old public key (g_0, g_1, u, v, μ, h) and secret key $(\widehat{x}_i, \widehat{y}_i)$ construct new public key $(\widehat{g}_0, \widehat{g}_1, u, v, \widehat{\mu}, h)$, where $\widehat{g}_0 = g_0^{1/(\gamma+\widehat{x}_i)}$, $\widehat{g}_1 = (g_1/\widehat{PK}_i)^{(1/(\gamma+\widehat{x}_i))}$, $\widehat{\mu} = (\widehat{g}_1)^{\gamma}$, and $g_0, g_1 \in G$. More precisely,

$$\begin{aligned}
\widehat{g}_0 &\longleftarrow \varphi\left(\widehat{A}_i^*\right) = g_0^{1/(\gamma+\widehat{x}_i)}, \\
\widehat{g}_1 &\longleftarrow \widehat{A}_i^* = \left(\frac{g_1}{\widehat{PK}_i}\right)^{1/(\gamma+\widehat{x}_i)}, \\
\widehat{\mu} &\longleftarrow \left(\frac{g_1}{\widehat{PK}_i}\right) \cdot \left(\widehat{A}_i^*\right)^{-\widehat{x}_i} = \left(\frac{g_1}{\widehat{PK}_i}\right)^{1-(\widehat{x}_i/\gamma+\widehat{x}_i)}, \\
&= \left(\widehat{A}_i^*\right)^{\gamma}, \\
&= (\widehat{g}_1)^{\gamma}.
\end{aligned} \tag{19}$$

Hence, the new secret key of the vehicle is $(\widehat{x}_i, \widehat{y}_i)$, and A_i updates to $\widehat{A}_i^*$. The new public key $(\widehat{g}_0, \widehat{g}_1, u, v, \widehat{\mu}, h)$ is broadcast by TA.

5. Security Analysis and Comparison

In this section, we will show that the proposed scheme satisfies the security requirements of VANETs and compare the security with other schemes.

5.1. Security Analysis

5.1.1. Authentication. The receiver can identify the invalid vehicles by verifying the signature of the messages. The generation of signature requires the secret key (x_i, y_i) and A_i of the sender, where (A_i, x_i) is an SDH pair.

Given the public parameters $(g_0, g_1, u, v, \mu, h, H)$, and for any vehicle with secret key (x_i, y_i) and A_i, the registration algorithm employed in the TA guarantees that $A_i^{\gamma+x_i} \cdot PK_i = g_0$, so (A_i, x_i) is an SDH tuple for $\mu = g_1^{\gamma}$. A correct group signature σ of message M signed with secret key (x_i, y_i) and A_i as equation (6) is proved to be correct by testing equation (12).

Our protocol is supported by honest-verifier zero-knowledge proof of an SDH pair under the DL assumption. Due to the fact that SDH problem is hard, the adversary cannot get (x_i, y_i) and generate a valid signature.

5.1.2. Privacy. The identity of the vehicle is fully-anonymous. The vehicle only broadcasts the signature σ of messages and publishes public key (g_0, g_1, u, v, μ, h), and the signature or public key does not carry any information concerning the identity of the sender. The private key (x_i, y_i) is computationally hard to derive from A_i or the transcript under SDH problem. It is computationally hard to derive identity information of the message sender from the signature σ. In addition, the real identity of the vehicle is bound to A_i (updated as partial secret key y_i is updated) and managed by the TA, which is of very high security. Therefore, the privacy information of the vehicle is protected.

5.1.3. Traceability. The real identity of the vehicle is fully-traceable. The vehicle can be tracked by the tracing key. As equation (18) does, TA can reveal the vehicle's identity by computing $A_i = T_3/(T_1^{\alpha} \cdot T_2^{\beta})$, which is bound to the real identity of the vehicle using the tracing key (α, β). The adversary cannot track the vehicles by analyzing the signature, as for the tracing key (α, β) cannot be derived under the decision linear problem.

5.1.4. Unlinkability. The vehicle signs message with private keys (x, y) which cannot be derived from the public key under SDH assumption. Each signature is generated by session keys $a, b \in_R \mathbb{Z}_p$ and private keys (x, y). Even the public key has not been updated for a long time, each signature will not be the same because of the helper value $(s_\alpha, s_\beta, s_x, s_y, s_{\delta_1}, s_{\delta_2})$ generated by session keys. The security of the session key is guaranteed by the linear encryption. The receiver cannot derive A_i related to the real identity of a vehicle from the signature. Due to the randomness of session keys (a, b), no adversary could link two anonymous identifiers or two different signatures $\sigma_1 \neq \sigma_2$ generated by the same vehicle. Furthermore, vehicle can regularly update its partial secret key y_i locally, so the identity binder A_i gets updated as well.

5.1.5. Exculpability. Exculpability requests that the private key is only known to herself.

TA generates a tracing key (α, β) and a partial key x_i for the vehicle in the system initialization phase and vehicle registration phase, respectively. The vehicle generates partial key y_i for herself. The partial key x_i is an exponent of SDH tuple (A_i, x_i). The partial key y_i is an exponent of public key PK_i.

TA cannot derive the secret key y_i of vehicle from PK_i under DL assumption. So TA does not have the signing key (x_i, y_i) of vehicle to sign the message for it. The strong exculpability is thus achieved.

5.2. Comparison. In this subsection, we compare the security of our scheme with other schemes from the following aspects and are listed in Table 2.

We reduce the credibility of RSUs in our scheme. As external devices, RSUs are vulnerable to geographic attacks. But the scheme of Funderburg and Lee [6] set the RSUs to be semitrusted devices, the leader-RSU would know the real identity of the vehicle in Lim et al.'s scheme [20], and Shim's scheme [4] also treats RSUs as trusted devices and exposes the real identity of the vehicle to the trace authority (TRA).

Table 2: Comparison of our scheme to others.

Schemes	[4]	[5]	[10]	[20]	[7]	[6]	Ours
Real ID exposure level	TRA	TA	TRC	Leader-RSU	GM	TA	TA
Pseudo-ID untraceable	No	No	—	Yes	Yes	Yes	Yes
Untrusted RSUs	No	No	No	No	No	Semi	Yes
Unlinkability	No	Yes	Yes	Yes	Yes	Yes	Yes
Private key update online	No	No	Yes (TRC)	Yes (GM)	Yes (GM)	Yes (TA)	Yes (V)
Tracing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Member revocation	PKG	TA	TA	Partial	GM	TA	TA
Exculpability	No	No	Yes	No	No	No	Yes

Table 3: The notation of the execution time of cryptography operations.

Notation	Description
T_{bp}	A bilinear pairing operation $e(P,Q)$, where $P,Q \in G$
T_{smbp}	Pairing-based scale multiplication operation $s \cdot P$, where $s \in Z_q^*, P \in G$
T_{pmbp}	Pairing multiplication operation $e(P_1,Q_1)e(P_2,Q_2)$, where $P_1,P_2,Q_1,Q_2 \in G$
T_{pabp}	Pairing-based point addition operation $P+Q$, where $P,Q \in G$
T_{htp}	Paring-based hash-to-point operation where H: $\{0,1\}^* \longrightarrow G$
T_{smecc}	ECC-based scale multiplication operation $x \cdot P$ where $x \in Z_q^*, P \in G$
T_{paecc}	ECC-based point addition operation $P+Q$ where $P,Q \in G$
T_h	One-way hash function operation

To prevent malicious tracking of vehicles by pseudo-identity, we implemented our protocol by short group signature technology. The ID-based schemes [4, 5] will expose the PID of the vehicle in the wireless environment. As for [10], the real-ID of vehicle is bound to public key.

The manager of vehicle's key decides when the key gets updated and the revocation of the group members. In our scheme, the signing key of the vehicle consists of two parts: the partial key distributed by TA and the partial key generated by the vehicle itself. The group signature-based schemes [6, 7, 20] cannot update the signing key by the vehicle instead by the group manager (GM) or TA. The ID-based schemes [4, 5] would update the key of the vehicle offline or by a secure channel. Unfortunately, Lim et al.'s [20] scheme cannot revoke the new member of a group. The scheme [10] entrusts the task of a session key update to the TRC (transportation regulation centre), which has great burden, and it is difficult to update the vehicle key in real-time.

Our scheme is designed by applying double key approach, so the global manager TA does not know the full signing key of the vehicle. The strong exculpability is met in this paper and the vehicle cannot deny the signature signed by itself, while other schemes [4–7, 20] cannot achieve this goal.

6. Performance

In this section, we analyze the performance of our scheme along with the existing relevant schemes [4–7, 10, 20].

Firstly, we define some notations of cryptography operations, as shown in the Table 3.

We compute the execution time of the cryptographic operations shown in Table 3 using a well-known library MIRACL [21]. The high-level interface to pairing functions is Type 1 pairings whose parameter of pairing-friendly curve (PFC) is defined in the class PFC.

Table 4: The execution time of cryptography operations, which is the average of 1000 times for every operation. The hardware platform is on the windows 10 operating system, and its CPU is Intel (R) Core (TM) i7-5500u with 8 gigabytes of memory.

Cryptography operations	Execution time (milliseconds)
T_{bp}	11.1991
T_{smbp}	3.5039
T_{pmbp}	11.6208
T_{pabp}	0.0295
T_{htp}	0.1202
T_{smecc}	0.0010
T_{paecc}	0.0011
T_h	0.0017

The hardware platform is on the windows 10 operating system, and its CPU is Intel (R) Core (TM) i7-5500u with 8 gigabytes of memory. The measurement results are listed in Table 4, which is the average of 1000 times for every operation.

The computation cost of the message signing, the single verification of a message, and the batch verification of multiple messages with relevant schemes [4–7, 10, 20] are compared in Table 5.

As illustrated in Table 5, due to the high time complexity of bilinear pairing, the rate [4, 6, 7, 20] is generally lower than that of ID-based schemes [5, 10]. But compared with other relevant schemes, the rate of our scheme is almost the same as that of other schemes [6, 7, 20], which is based on short group signatures [9]. It is worth mentioning that our scheme meets higher security requirements. The security of

Table 5: The computation cost of the routine.

Schemes	Signing	Single verification	Batch verification
[4]	$3T_{\text{smbp}} + 2T_{\text{pabp}} + T_h \approx 10.5724\,ms$	$3T_{bp} + 2T_{\text{smbp}} + T_{\text{pabp}} + 2T_h \approx 40.6380\,ms$	$3T_{\text{bp}} + (n+1)T_{\text{smbp}} + 3(n-1)T_{\text{pabp}} + 2nT_h \approx 3.5958n + 37.0127\,(ms)$
[5]	$3T_{\text{smecc}} + 3T_h \approx 0.0041\,ms$	$3T_{\text{smecc}} + 2T_h + 2T_{\text{paecc}} \approx 0.0086\,ms$	$(n+2)T_{\text{smecc}} + (3n-1)T_h + 2nT_{\text{paecc}} \approx 0.0083n + 0.0003\,(ms)$
[10]	$4T_{\text{smbp}} + T_{\text{pabp}} \approx 14.0451\,ms$	$2T_{\text{bp}} + T_{\text{smbp}} + T_{\text{pabp}} \approx 25.9316\,ms$	$2T_{bp} + T_{\text{smbp}} + (2n+1)T_{\text{pabp}} \approx 0.059n + 25.9316\,(ms)$
[6]	$2T_{\text{pmbp}} + T_{\text{htp}} \approx 23.3618\,ms$	$4T_{\text{pmbp}} + T_{\text{htp}} \approx 46.6035\,ms$	$4nT_{\text{pmbp}} + nT_{\text{htp}} \approx 46.6035n\,(ms)$
[7]	$2T_{\text{pmbp}} + 2T_{\text{htp}} \approx 23.4820\,ms$	$4T_{\text{pmbp}} + 2T_{\text{htp}} \approx 46.7237\,ms$	$4nT_{\text{pmbp}} + 2nT_{\text{htp}} \approx 46.7237n\,(ms)$
[20]	$2T_{\text{pmbp}} + T_{\text{htp}} \approx 23.3618\,ms$	$4T_{\text{pmbp}} + T_{\text{htp}} \approx 46.6035\,ms$	$4nT_{\text{pmbp}} + nT_{\text{htp}} \approx 46.6035n\,(ms)$
Ours	$3T_{\text{pmbp}} + T_{\text{htp}} \approx 34.9826\,ms$	$5T_{\text{pmbp}} + T_{\text{htp}} \approx 58.2243\,ms$	$5nT_{\text{pmbp}} + nT_{\text{htp}} \approx 58.2243n\,(ms)$

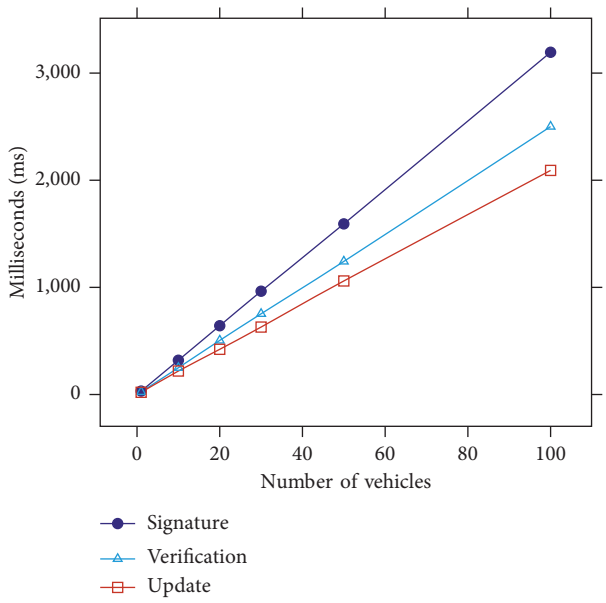

Figure 2: Approximate time required for signature, verification, and update processes.

exculpability cannot be achieved in [6, 7, 20] which were based on short group signatures.

Our protocol is simulated on the windows 10 operating system, and its CPU is Intel (R) Core (TM) i7-5500u with 8 gigabytes of memory. We compute the execution time of the routine of the signature process, verification process, and key update process using cryptographic library MIRACL and the performance is shown in Figure 2.

As illustrated in Figure 2, each signature signed by vehicle takes less than 32 ms. The process of message verification takes about 25 ms, and the keys can be updated within 21 ms approximately.

7. Conclusion

In this paper, we propose a privacy-preserving authentication scheme for VANETs with strong exculpability. By using the double key approach and short group signature, vehicles update their private key online and establish trusted communication with TA and RSUs. We also showed the strong security property of our scheme regarding the message authentication, anonymity, traceability, unlinkability, and strong exculpability. We further compared with other relative schemes and showed our advantages, regarding the execution efficiency and the security properties.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partly supported by the Fundamental Research Funds for the Central Universities under Grant no. 30106220482.

References

[1] M. S. Sheikh and J. Liang, "A comprehensive survey on VANET security services in traffic management system," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 2423915, 2019.

[2] FCC, "Dedicated short range communications (DSRC) service," 2022, https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service.

[3] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular Ad hoc network and vehicle cloud computing: a survey," *Wireless Communications and Mobile Computing*, vol. 2020, no. 3, Article ID 5129620, pp. 1–25, 2020.

[4] K. A. Shim, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012.

[5] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular Ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[6] L. E. Funderburg and I. Y. Lee, "A privacy-preserving key management scheme with support for sybil attack detection in VANETs," *Sensors*, vol. 21, no. 4, p. 1063, 2021.

[7] Q. Wang, D. Gao, C. H. Foh, and C. M. L. Victor, "An edge computing-enabled decentralized authentication scheme for vehicular networks," in *Proceedings of the IEEE International Conference on Communications (ICC)*, IEEE, Dublin, Ireland, June 2020.

[8] G. Ateniese, J. Camenisch, and M. Joye, "A practical and provably secure coalition-resistant group signature scheme," in *Proceedings of the 20th Annual International Cryptology Conference*, Springer-Verlag, Santa Barbara, CA, USA, August 2000.

[9] B. Dan, X. Boyen, and H. Shacham, "Short group signatures," in *Proceedings of the Annual International Cryptology Conference*, Springer, Berlin, Heidelberg, July 2004.

[10] B. Samra and F. Semchedine, "A certificateless ring signature scheme with batch verification for applications in VANET," *Journal of Information Security and Applications*, vol. 55, 2020.

[11] B. Samra and S. Fouzi, "New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET," *Vehicular Communications*, vol. 34, 2022.

[12] B. Cronin, "Vehicle based data and availability," 2021, https://www.its.dot.gov/itspac/october2012/PDF/data_availability.pdf.

[13] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "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.

[14] K. K. Chauhan, S. Kumar, and S. Kumar, "The Design of a Secure Key Management System in Vehicular Ad Hoc networks," in *Proceedings of the Conference on Information and Communication Technology*, Gwalior, India, November 2017.

[15] C. Zhang, R. Lu, and X. Lin, "An efficient identity-based batch verification scheme for vehicular sensor networks," in

Proceedings of the 27th Conference on Computer Communications, Phoenix, AZ, USA, April 2008.

[16] G. Ateniese and G. Tsudik, "Some open issues and directions in group signatures," in *Proceedings of the Financial Cryptography 1999*, pp. 196–211, Springer-Verlag, Berlin, Germany, Febuary 1999.

[17] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: formal defini- tions, simplified requirements, and a construction based on general assumptions," in *Proceedings of the Eurocrypt 2003*, pp. 614–629, Springer-Verlag, Berlin, Germany, May 2003.

[18] Giuseppe Ateniese, C. Jan, M. Joye, and G. Tsudik, "A practical and provably secure coalition- resistant group signature scheme," in *Proceedings of the Crypto 2000*, pp. 255–270, Springer-Verlag, Berlin, Germany, August 2000.

[19] B. Dan and H. Shacham, "Group signatures with verifier-local revocation," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, Washington, DC, USA, October 2004.

[20] K. Lim, W. Liu, X. Wang, and J. Joung, "SSKM: scalable and secure key management scheme for group signature based authentication and CRL in VANET," *Electronics*, vol. 8, no. 11, p. 1330, 2019.

[21] Shamus Software Ltd, "MIRACL Library," 2015, https://www.shamus.ie/index.php?page=home.