Hindawi
Complexity
Volume 2024, Article ID 9840567, 1 page
https://doi.org/10.1155/2024/9840567

Retraction

Retracted: An Anonymous Authentication Scheme in VANETs of Smart City Based on Certificateless Group Signature

Complexity

Received 23 January 2024; Accepted 23 January 2024; Published 24 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Zheng, G. Chen, and L. Guo, "An Anonymous Authentication Scheme in VANETs of Smart City Based on Certificateless Group Signature," *Complexity*, vol. 2020, Article ID 1378202, 7 pages, 2020.

Hindawi
Complexity
Volume 2020, Article ID 1378202, 7 pages
https://doi.org/10.1155/2020/1378202

Research Article

An Anonymous Authentication Scheme in VANETs of Smart City Based on Certificateless Group Signature

Yuanpan Zheng,[1,2] **Guangyu Chen**,[1] **and Liguan Guo**[3]

[1]*School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450001, China*
[2]*Henan Province Engineering Laboratory for Information Technology of Emergency Platform, Zhengzhou 450001, China*
[3]*Henan Xinanli Security Technology Co., Ltd., Zhengzhou 450001, China*

Correspondence should be addressed to Yuanpan Zheng; ypzheng@zzuli.edu.cn

Received 28 March 2020; Revised 13 May 2020; Accepted 27 May 2020; Published 29 June 2020

Guest Editor: Zhihan Lv

With the change of the network communication environment in vehicular ad hoc networks (VANETs) of a smart city, vehicles may encounter security threats such as eavesdropping, positioning, and tracking, so appropriate anonymity protection is required. Based on the certificateless cryptosystem and group signature ideas, this paper proposes a certificateless group signature anonymous authentication scheme for the VANETs of a smart city. In this scheme, it can implement the process of adding, signing, verifying, and revoking group members only by simple multiplication of the elliptic curve and synchronization factor technology, which shortens the length of the signature and improves the efficiency of the signature. From the proofs of correctness and security, we know that it does not only has anonymity and traceability of the group signature scheme but also has unforgeability and forward security. According to the performance verification, this scheme has lower calculation overhead and higher authentication efficiency.

1. Introduction

Vehicular ad hoc networks (VANETs) [1] of a smart city, as a typical application of the Internet of Things technology, enable real-time traffic information interaction between vehicles and vehicles and between vehicles and the infrastructure. And, it has played a positive role in reducing traffic accidents and has been widely developed in the field of intelligent transportation. With the continuous change of the network environment, a variety of information security and privacy leakage issues have also emerged, seriously threatening the personal safety and personal privacy of vehicle users. Therefore, it is necessary to provide corresponding security policies, which can effectively protect the communication security and personal privacy of vehicle users while providing fast services for vehicle users.

At present, anonymous authentication technologies in VANETs mainly include PKI-based authentication, identity-based authentication, and group signature-based authentication. In the early days, the public key infrastructure- (PKI-) based public key certificate scheme proposed by Raya and Hubaux [1] in 2007 was mainly used. This scheme requires a large number of public-private key pairings and related certificates to be stored in the vehicles. By occupying a large amount of storage space, it increases communication and computational overheads and causes certificate management problems. Shim [2] proposed an identity-based batch authentication scheme. The scheme uses a pseudonym to represent vehicle identity information and uses a pseudonym replacement strategy for each message signature to achieve message traceability. However, in this scheme, PKG knows the private keys of all users, so it is inevitable that the key escrow problem will occur.

In 1991, Chaum and Heyst [3] first proposed the concept of the group signature. It allows group members to sign anonymously on behalf of the group. The group administrator is responsible for the creation and distribution of group member keys. The group members use group member

certificates to sign on messages. The group public key is used to verify its authenticity. The verifier can only verify that the signer is from a member of the group but cannot determine the identity of specific members in the group, thereby protecting the group members' identity. In addition, the group administrator can open the signature and reveal the true identity of the signing members to resolve the dispute. But, it is computationally infeasible to distinguish whether two different group signatures come from the same signer. Therefore, the group signature technology has been widely used, and it has been gradually introduced into the anonymous authentication scheme in VANETs [4–7]. Shao et al. [5] proposed a threshold anonymous authentication protocol capable of implementing batch authentication based on the group signature. Zheng et al. [6] introduced a lightweight group signature technology, which made the group public key and signature length fixed and did not depend on the number of group members. Zhao [7] proposed a revocable group signature scheme based on the Chinese remainder theorem in VANETs. When members join and revoke, they only need to regenerate a new group public key without changing the key pairings of other members, improving the efficiency of member joining and revoking. However, in these schemes, each member needs to generate a corresponding group member certificate, which will increase storage overhead and computational overhead.

In 2003, Al-Riyami and Paterson [8] first proposed a certificateless cryptosystem. In the system, a part of the user key is provided by the key generation center and the rest is generated by the user to form the user key, which ensures that the key generation center does not know all the user's private keys, and it solves the problem of certificate management in traditional public key cryptosystems and key escrow in identity-based cryptosystems. Based on the group signature technology, Chen et al. [9] and Li et al. [10] proposed different certificateless group signature schemes. At the same time, certificateless group signature schemes applied to VANETs have also been proposed [11–17], which has also become a hotspot in the security of VANETs. Zhang et al. [12] and Chen et al. [14] used bilinear pairings to study the application of the certificateless group signature in VANETs, avoiding the problem of key escrow, without the need for certificate management, effectively reducing the system storage load.

However, the current certificateless group signature schemes are implemented with the help of bilinear pairing operations, which increases the overhead of the system operation. Therefore, this paper proposes a certificateless group signature scheme based on elliptic curves, which uses elliptic curves instead of bilinear pairings for operations. This scheme not only inherits the security and anonymity of group signature schemes but also greatly reduces the computational overhead. In particular, the introduction of the synchronization factor technology in this scheme makes it unnecessary to modify the public key information of the group administrator when the members in the group change. Only the group synchronization factor and group members' synchronization factor are calculated and modified, which greatly reduces the calculation steps when group members join and revoke.

2. Preliminaries

2.1. System Model. In the general mode, the system model of VANETs consists of fixed RSUs (road side units) at the road side, mobile OBUs (on-board units) equipped in vehicles, and a TA (trusted authority), as shown in Figure 1.

OBUs access the VANETs through the road side deployment infrastructure RSUs and periodically broadcast their own vehicle information to other vehicles, including safety information such as the location, speed, direction, acceleration, road conditions, traffic events, and time stamps, so that other OBUs can quickly obtain useful information on the road. RSUs can broadcast and receive some signature information in the group and provide various services for the OBUs. And, when needed, they reveal the real identification of some illegal vehicles and broadcast the identification information of revoked vehicles. RSUs have their own storage space and computing capabilities. The TA, as a third-party trusted agency in this scheme, saves the real identity information of OBUs and RSUs and generates public and private key pairings of OBUs and RSUs for identification in VANETs.

2.2. Elliptic Curve. The elliptic curve is an encryption algorithm in the current public key encryption system, and it is also the encryption algorithm that can provide the highest encryption strength for data. The encryption strength corresponding to the encryption calculation using the 160-bit key length is equivalent to the encryption length corresponding to the RSA algorithm using the 1024-bit key length in the public key encryption system. However, the elliptic curve has the characteristics of fewer calculation parameters, shorter key length, and faster operating speed. Therefore, it is appropriate to apply the elliptic curve encryption algorithm to the VANETs with limited computing capacity, storage space, and transmission bandwidth.

Definition 1 (elliptic curve definition). This scheme uses a 160-bit elliptical encryption algorithm. Assume that q is a large prime number and F_q is a finite field of the module q. An elliptic curve over a finite field F_q can be defined as: E: $y^2 \equiv x^3 + ax + b (\mathrm{mod} q)$, where $a, b, x,$ and $y \in F_q$ and $\Delta = 4a^3 + 27b^2 \neq 0$.

Definition 2 (addition of elliptic curves). Assume that the point of an elliptic curve $P = (x_1, y_1) \in E$, $-P = (x_1, -y_1)$ is the negative point of P, $Q = (x_2, y_2) \in E, Q \neq -P$, the line l passes through P and Q, and it intersects the elliptic curve at a point $R' = (x_3, -y_3)$, The symmetrical point about the x-axis with R' is $R = (x_3, y_3)$ and $R = P + Q$. The addition cyclic group of the prime order q on the elliptic curve E is $G_q = \{(x, y)\colon a, b, x, y \in F_q, (x, y) \in F_q, (a, b)\}$ where G is a generator on the elliptic curve E and the scalar multiplication operation on the elliptic curve is $kP = P + P + P + \cdots + P (k, k \in Z_q^*)$.

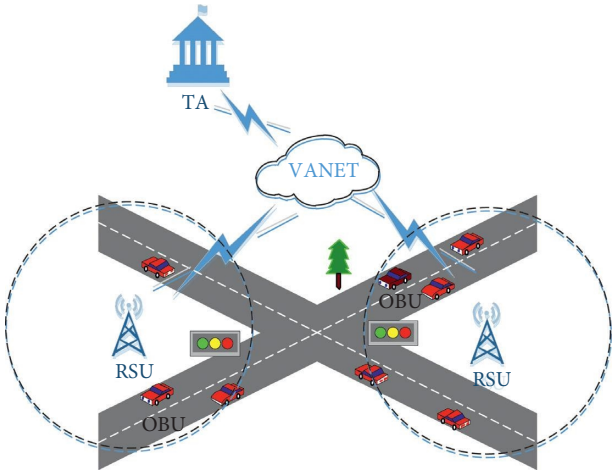

Figure 1: The system model of VANETs.

Definition 3 (elliptic curve discrete logarithm problem (ECDLP)). There are two points P_1 and P_2 on the elliptic curve E on the finite field F_q and there exists $k \in Z_q^*$, such that $P_1 = kP_2$; it is feasible to calculate P_1 from k and P_2, but it is not advisable to calculate k from P_1 and P_2.

3. Establishment of an Anonymous Authentication Scheme Based on Certificateless Group Signature

Design Idea. In this paper, the certificateless design idea is integrated into the scheme based on the group signature, which simplifies the member joining process and can resist public key replacement attacks. During the member joining process, the member A uses the private key to sign SK_A, obtains the identity signature information h_A, and sends $(ID_A \| Y_A \| h_A \| v_A \| b_A)$ to RSU and RSU obtains A's public key from TA to verify the identity information sent by A. It not only proves the legitimacy of A but also avoids public key replacement attacks. In addition, in the process of generating the group member certificate, the vehicle user needs to verify the identity of the group administrator RSU before accepting the member certificate to enhance the credibility of the certificate.

The certificateless group signature anonymous authentication scheme includes system initialization, public and private key generation for group administrators and group members, group member joining, signature generation, signature verification, member revocation, and opening signature. The specific work is as follows:

(1) *System Initialization.* TA chooses the system parameters and generates the master key and its own public key, and public key information is made public.

(2) *Public and Private Key Generation for Group Administrators and Group Members.* TA generates relevant public and private keys for administrators RSU and vehicle users OBU. The administrator generates an initial group synchronization factor T.

(3) *Member Joining.* The new member A joins according to the group joining method and generates a self-synchronization factor and updates the group synchronization factor.

(4) *Signature Generation.* Group member A signs the message M based on the signature algorithm.

(5) *Signature Verification.* In VANETs, the verifier verifies the message signature through making information and signature information public and confirms that the signed message is signed and issued by a member of the group.

(6) *Member Revocation.* When a member in the group leaves the group for some reason, RSU recalculates the synchronization factor $T\prime$ in the group according to the identity information of the member A which left the group and sends the new synchronization factor $T\prime$ and related information of A's synchronization factor to other members B in the group, which updates their synchronization factor to T_B according to the information.

(7) *Opening Signature.* When A finds that the message signature sent by the group member vehicle user is false information or a dispute occurs between the group members, the signature is calculated by opening the signature to reveal the identity of the user.

4. Proposed Scheme

4.1. Initialization. Based on the selected security parameter k, TA generates two large prime numbers p and q, such that $q|p-1$. Choose the generator P on the cyclic group G on the elliptic curve of the order q. Then, choose two collision-free hash functions: $H: \{0,1\}^* \longrightarrow Z_q^*$ and $H_1: \{0,1\}^* \times G \longrightarrow Z_q^*$. TA chooses a random parameter $z \in Z_q^*$ as the system master key and calculates $P_z = zP$ as the public key. TA makes system parameters $\text{params} = \{p, q, G, P, P_z, H, H_1\}$ public and secretly saves the system master key z.

4.2. Public and Private Key Generation

(1) In this scheme, RSU acts as a group manager to manage vehicle members in the group. Assume that the identity information of the group manager RSU is ID_{RSU}, then RSU randomly chooses $x_{\text{RSU}} \in Z_q^*$, calculates $P_{\text{RSU}} = x_{\text{RSU}}P$, and sends $P(ID_{\text{RSU}}, P_{\text{RSU}})$ to TA; TA randomly chooses $r_{\text{RSU}} \in Z_q^*$, calculates $R_{\text{RSU}} = r_{\text{RSU}}P$ and $S_{\text{RSU}} = r_{\text{RSU}} + zH_1(ID_{\text{RSU}} \| P_{\text{RSU}} \| R_{\text{RSU}})$, and sends $(R_{\text{RSU}}, s_{\text{RSU}})$ to RSU secretly, where R_{RSU} is a partial public key of RSU and s_{RSU} is a partial private key of RSU; RSU receives the information, verifies whether $s_{\text{RSU}}P = R_{\text{RSU}} + P_z H_1(ID_{\text{RSU}} \| P_{\text{RSU}} \| R_{\text{RSU}})$ is established, and judges the validity of the partial private key s_{RSU}. At this time, RSU gets a complete private key pairing $SK_{\text{RSU}} = (x_{\text{RSU}}, s_{\text{RSU}})$ and a complete public key

pairing $PK_{RSU} = (x_{RSU}P, s_{RSU}P) = (P_{RSU}, S_{RSU})$. TA saves the corresponding information $(ID_{RSU}, P_{RSU}, S_{RSU}, s_{RSU})$ of RSU and saves the public key to the public list.

(2) Assume that the identity information of the user OBU_A is ID_A. Through the above process, the private key pairing $SK_A = (x_A, s_A)$ and the public key pairing $PK_A = (P_A, S_A)$ of the user OBU_A are generated, and the public key PK_A is made public. The hash function H_1 is used to generate a part of the private key.

(3) The group manager RSU randomly chooses $e \in Z_q^*$ and calculates $T_0 = eP$ as the initial group synchronization factor of the group, and the engaged synchronization factor is T.

4.3. Joining

(1) When the user OBU_A wants to join the group, OBU_A randomly chooses $y_A \in Z_q^*$ and $b_A \in Z_q^*$ and calculates $Y_A = y_A P$, $h_A = H(ID_A \| PK_A \| Y_A \| b_A)$, and $v_A = y_A - h_A \cdot SK_A$. The user OBU_A sends $(ID_A \| Y_A \| h_A \| v_A \| b_A)$ to RSU.

(2) RSU sends ID_A to TA, obtains OBU_A's public key PK_A, verifies that whether $Y_A' = v_A P + h_A PK_A = Y_A$ is established, and generates a certificate for OBU_A if it holds.

(3) RSU randomly chooses $e_A \in Z_q^*$, calculates $E_A = Y_A + e_A P = (e_A + y_A)P$, $h_{RSU} = H(E_A \| PK_{RSU} \| T)$, and $s_{RSU} = e_A + SK_{RSU} \cdot h_{RSU}$, sends $(E_A, h_{RSU}, s_{RSU}, T)$ to OBU_A, and stores $(ID_A, PK_A, Y_A, b_A, E_A, E_A P, e_A, h_A, s_A)$ into the group member information list.

(4) OBU_A verifies RSU's public key PK_{RSU} and calculates that whether $E_A' = (s_{RSU} + y_A)P - h_{RSU} PK_{RSU} = E_A$ is established. If it holds, the user OBU_A joins the group and generates the group member certificate as $(ID_A, PK_{RSU}, Y_A, E_A, b_A, T)$.

(5) RSU sends (T, b_A) to other members in the group, and member OBU_B updates their synchronization factor T_B. Assuming that OBU_B's certificate is $(ID_B, PK_{RSU}, Y_B, E_B, b_B, T_B)$, OBU_B calculates a new synchronization factor as $T_B' = T + T_B(b_B - b_B)$, and OBU_B's new certificate is $(ID_B, PK_{RSU}, Y_B, E_B, b_B, T_B')$.

(6) RSU updates the synchronization factor as $T\prime = T \cdot (b_A + x_{RSU})$.

4.4. Other Steps. The remaining four steps in the scheme are, in order, signature generation, signature verification, member revocation, and signature opening.

4.4.1. Signature Generation. Assume that the group member OBU_A generates a signature on message M, calculates $C_1 = E_A P + T_A PK_{RSU}$ and $C_2 = T_A P$, $C_3 = b_A E_A$, randomly chooses $r_1, r_2, r_3, r_4 \in Z_q^*$, and calculates $d_1 = r_1 C_1 - r_2 PK_{RSU}$, $d_2 = r_1 C_2 + r_3 S_{RSU}$, $d_3 = r_3 P$, $d_4 = r_3 PK_{RSU} + r_4 P$, $c = H(PK_{RSU} \| M \| C_1 \| C_2 \| C_3 \| d_1 \| d_2 \| d_3 \| d_4)$, $s_1 = r_1 - cb_A$, $s_2 = r_2 - cb_A T_A$, $s_3 = r_3 - cT_A$, and $s_4 = r_4 - cE_A$; the output signature is $RM = (c, s_1, s_2, s_3, s_4, C_1, C_2, C_3)$.

4.4.2. Signature Verification. The verifier calculates $d_1' = s_1 C_1 - s_2 PK_{RSU} + cPC_3$, $d_2' = s_1 C_2 + s_3 S_{RSU} + cTP$, $d_3' = s_3 P + cC_2$, $d_4' = cC_1 + s_4 P + s_3 PK_{RSU}$, and $c\prime = H(PK_{RSU} \| m \| C_1 \| C_2 \| C_3 \| d_1' \| d_2' \| d_3' \| d_4')$ based on $(c, s_1, s_2, s_3, s_4, C_1, C_2, C_3)$. If the equation $c\prime = c$ holds, the verification passes.

4.4.3. Member Revocation. To revoke the user OBU_A, RSU calculates a new synchronization factor $T\prime = T \cdot (b_A + x_{RSU})^{-1}$ based on (T, b_A). Then, RSU sends $(T\prime, b_A)$ to other members in the group OBU_B, and OBU_B updates their synchronization factor T_B to T_B', where $T_B' = (T_B - T\prime) \cdot (b_A - b_B)^{-1}$.

4.4.4. Signature Opening. When RSU finds that the message signature sent by the group member vehicle user is false information or a dispute occurs between the group members, it calculates $E_A P = C_1 - C_2 SK_{RSU}$ based on the signed message $RM = (c, s_1, s_2, s_3, s_4, C_1, C_2, C_3)$ and the group manager's private key $SK_{RSU} = (x_{RSU}, s_{RSU})$ and then finds the corresponding identity of the group member.

5. Anonymous Scheme Analysis

5.1. Correctness Analysis

5.1.1. Correctness of Key Distribution. After the group manager RSU receives (R_{RSU}, s_{RSU}), it verifies whether $s_{RSU}P = R_{RSU} + P_z H_1(ID_{RSU} \| P_{RSU} \| R_{RSU})$ is established. Since $s_{RSU}P = r_{RSU}P + zPH_1(ID_{RSU} \| P_{RSU} \| R_{RSU}) = R_{RSU} + P_z H_1(ID_{RSU} \| P_{RSU} \| R_{RSU})$, the verification result is consistent with the result of the signature generation algorithm, so the signature scheme satisfies the correctness.

Similarly, after the user OBU_A receives OBU_A, it verifies whether $s_A P = R_A + P_z H_1(ID_A \| P_A \| R_A)$ is established. Since $s_A P = r_A P + zPH_1(ID_A \| P_A \| R_A) = R_A + P_z H_1(ID_A \| P_A \| R_A)$, the signature scheme satisfies the correctness.

5.1.2. Correctness of Signature in Joining. After RSU receives the signature information $(ID_A \| Y_A \| h_A \| v_A \| b_A)$ from the user OBU_A, if (h_A, v_A) is a legitimate signature, the equation $Y_A' = v_A P + h_A PK_A = y_A P - h_A SK_A P + h_A PK_A = Y_A$ holds, and then RSU calculates $h_A' = H(ID_A \| PK_A \| Y_A' \| b_A)$ based on Y_A' and gets $h_A' = h_A$. And so, the $r_4 P - cE_A P + r_3 PK$ signature is valid, that is, the identity of the user OBU_A is valid.

Similarly, when OBU_A receives the message $(E_A, h_{RSU}, s_{RSU}, T)$ sent by RSU and calculates $E_A' = (s_{RSU} + y_A)P - h_{RSU} PK_{RSU}$ based on RSU's public key PK_{RSU} and

$s_{RSU} = e_A + SK_{RSU} \cdot h_{RSU}$, then the equation $E_A' = E_A$ holds. And so, the signature is valid.

5.1.3. Correctness of Group Signature. If $(c, s_1, s_2, s_3, s_4, C_1, C_2, C_3)$ is a legitimate signature, the verifier calculates $d_1' = s_1C_1 - s_2PK_{RSU} + cPC_3 = r_1C_1 - cb_AE_AP - cb_AT_APK_{RSU} - r_2PK_{RSU} + cb_AT_APK_{RSU} + cb_AE_AP = r_1C_1 - r_2PK_{RSU} = d_1$, $d_2' = s_1C_2 + s_3S_{RSU} + cTP = r_1C_2 - cb_AT_AP + r_3S_{RSU} - cT_AS_{RSU} + cTP = r_1C_2 + r_3S_{RSU} = d_2$, $d_3' = s_3P + cC_2 = r_3P - cT_AP + cT_AP = r_3P = d_3$, and $d_4' = cC_1 + s_4P + s_3PK_{RSU} = cE_AP + cT_APK_{RSU} + r_4P - cE_AP + r_3PK_{RSU} - cT_APK_{RSU} = r_3PK_{RSU} + r_4P = d_4$, based on $TP = T_A(b_A + x_{RSU})P = T_Ab_AP + T_AS_{RSU}$ and gets $c\prime = c$ from the existing public information, so the signature verification algorithm is correct.

5.2. Unforgeability. Unforgeability means that the group certificate of the members in the group is unforgeable.

In this scheme, RSU's private key pairing is $SK_{RSU} = (x_{RSU}, s_{RSU})$, where $s_{RSU} = r_{RSU} + zH_1(ID_{RSU} \| P_{RSU} \| R_{RSU})$; the group certificate for the group member OBU_A is $(ID_A, PK_{RSU}, Y_A, E_A, b_A, T_A)$, where $E_A = Y_A + e_AP = (e_A + y_A)P$, $Y_A = y_AP$, and the synchronization factor of the group T and the synchronization factor of the group member OBU_A have the following relationship: $T = T_A(b_A + x_{RSU})$. y_A, b_A, x_{RSU}, and e_A are private to group members OBU_A and RSU, respectively, so no single party can complete the group member certificate creation independently. Therefore, the group certificate is unforgeable.

5.3. Forward Security. When group member OBU_A joins the group, the group synchronization factor T is updated as follows: $T\prime = T \cdot (b_A + x_{RSU})$, based on b_A provided by OBU_A, and the synchronization factors of other members OBU_B in the group are updated as follows: $T_B' = T + T_B(b_B - b_B)$; when the group member OBU_A is revoked, the group synchronization factor T is updated as follows: $T\prime = T \cdot (b_A + x_{RSU})^{-1}$, and the synchronization factors of other members OBU_B in the group are updated as follows: $T_B' = (T_B - T\prime) \cdot (b_A - b_B)^{-1}$. It can be seen that the signature in the verification phase and the synchronization factor used in the verification phase will be updated synchronously according to the membership addition and revocation. After the update, the previous signature verification equation will not be established, so the forward security can be guaranteed.

5.4. Performance Analysis. In this section, performance analysis will be performed in terms of communication costs and calculation costs. For this scheme, the communication cost needs to consider the length of the group manager's public key and the length of the group member's signature. In the calculation aspect, the cost of joining the group, the cost of revoking the group, the cost of computing the signature, and the cost of verifying the signature are considered. Compared with other group signature schemes, some performance analysis comparisons are made as given in Table 1, where N represents the number of current group members and the number of joined and revoked members each time is set to 1.

In this scheme, the length of the group manager's public key and the length of the group member's signature information are not directly related to the number of members in the group and are constant.

In this scheme, when joining and revoking, the synchronization factor of each user needs to be updated, so the cost of joining and revoking is O (N).

In this scheme, the efficiency of the calculation cost of the information signature and the verification cost of the signature information are both constant, and the number of group members does not affect the time spent on signature and verification.

For this scheme, the performance analysis mainly considers the cost of group membership joining and revocation, the cost of information signature, and the cost of verifying signature information.

According to the literature [15], we choose a hardware platform consisting of Intel I7-6700 and Windows7 with 8G processor memory. By performing elliptic curve/bilinear pairing simulation experiments multiple times and taking the average value of the results, the operation execution schedule can be obtained as shown in Table 2. The comparison of this paper's average execution time of simulation operations is shown in Figure 2.

Considering the overall performance of the scheme, we will focus on analyzing the time overhead in the signature generation and signature verification process. This scheme is compared with the existing schemes [14, 15]. In the signature generation phase, scalar multiplication of bilinear pairs is mainly used in the scheme [14, 15]. The overall multiplication operation is less than this scheme, but the length of a single multiplication operation is longer than the elliptic curve multiplication and modular multiplication operations used in this scheme, and the overall time overhead is greater than the time overhead of this scheme; moreover, in the signature generation, the calculation of $2T_{EC\_MUL} + 2T_{MUL}$ is a fixed calculation, and it does not need to participate in each calculation process, which can further reduce the calculation cost of group members when performing signature generation. In the signature verification phase, the time-consuming bilinear operation in the scheme [14, 15] increases the time overhead, and the signature verification process of this scheme is not much different from the signature generation calculation overheads, as shown in Table 3. The comparison of signature generation and signature verification overhead for the three schemes is shown in Figure 3.

In the process of the group member joining, since the group members and the group management need to verify the identity of each other, the group members need to perform four elliptic curve multiplication operations and two hash comparisons. During the joining and revocation stages of group members, the group management broadcasts the synchronization coefficients of new members, and the members within the group update their respective

Table 1: Performance analysis.

Scheme	Length of public key	Signature length	Joining cost	Revocation cost	Signature cost	Verification cost
LPY [4]	O (1)	O (1)	O (N)	O (1)	O (1)	O (1)
YJD [11]	O (1)	O (1)	O (N)	O (1)	O ($N\log n$)	O (1)
This scheme	O (1)	O (1)	O (N)	O (N)	O (1)	O (1)

Table 2: Average execution time of simulation operations.

Symbol	Description	Execution time (ms)
T_{MC_MUL}	Multiplication on elliptic curves	0.3476
T_{MC_ADD}	Addition on elliptic curves	0.002
T_{MUL}	Modular multiplication	0.0119
T_H	General hash function operations	0.0012
T_{PB_SM}	Scalar multiplication	0.817
T_{PB}	Bilinear operation	5.5852

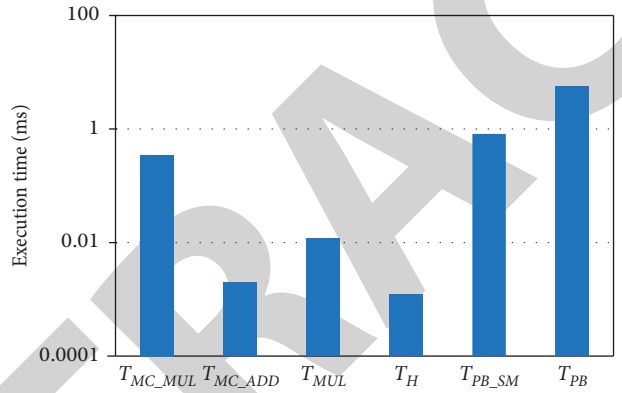

Figure 2: Comparison of average execution time of simulation operations.

Table 3: Signature generation and verification calculation overhead.

Scheme	Signature generation		Signature verification	
	Calculation overhead	Time overhead (ms)	Calculation overhead	Time overhead (ms)
Scheme [14]	$2T_{PB} + 1T_H + 10T_{PB\_SM}$	19.3416	$2T_{PB} + 1T_{PB\_SM}$	11.9874
Scheme [15]	$5T_{PB\_SM}$	4.085	$4T_{PB} + 2T_{PB\_SM}$	23.9748
This scheme	$4T_{MC\_MUL} + 12T_{MUL} + T_H$	1.5344	$4T_{MC\_MUL} + 7T_{MUL} + T_H$	1.4749

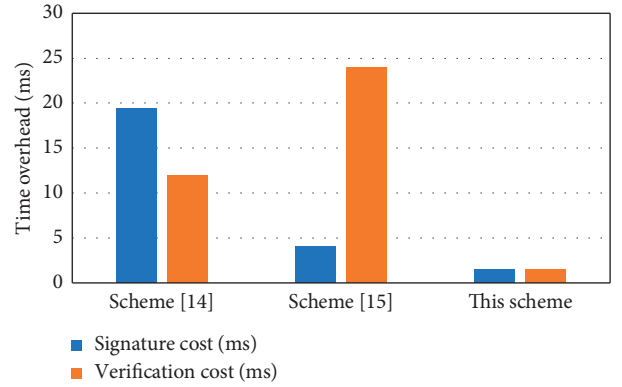

Figure 3: Comparison of signature generation and signature verification overhead.

synchronization factors. Without modifying the group public key, the calculation costs caused by changes in the members of the group will be spent, allocating sales to members in the group and reducing the calculation requirements for group management.

6. Conclusion

Aiming at the problem of low authentication efficiency in the anonymous authentication scheme in VANETs, this paper proposes a certificateless elliptic curve anonymous authentication scheme. Though based on a certificateless signature scheme, this scheme does not have to consider certificate maintenance and key escrow issues. It also uses elliptic curves to perform calculations on the basis of certificatelessness and introduces synchronization factor technology to further improve computing efficiency of group members when joining, revoking, and signing. The analysis of the scheme shows that the proposed scheme can not only ensure the anonymity and traceability of the group signature scheme but also ensure unforgeability and forward security under the premise of correctness. The partial key generation scheme adopted in this scheme effectively ensures the security of user keys, and there is no need to save too much certificate information in the system, and the calculation and storage overhead is low. Therefore, it is very suitable for OBUs and RSUs with very limited computing and storage space in the VANETs.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Natural Science Foundation of China (grant no. 51404216) and the Henan Province Programs for Science and Technology Development (grant nos. 202102210180, 172102310670, and 152102310374).

References

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

[2] K.-A. Shim, "Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree," *IEEE Transactions on Wireless Communications*, vol. 12, no. 11, pp. 5386–5393, 2013.

[3] D. Chaum and V. E. Heyst, "Group signatures," *Advances in Cryptology—EUROCRYPT'91*, Springer, Berlin, Germany, pp. 257–265, 1991.

[4] C. I. Fan, W. Z. Sun, S. W. Huang, W. Juang, and J. Huang, "Strongly privacy-preserving communication protocol for VANETs," in *Proceedings of the 2014 Ninth Asia Joint Conference on Information Security*, IEEE, Wuhan, China, September 2014.

[5] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.

[6] M. Zheng, Y. Duan, and H. Lyu, "Research on identity authentication protocol group signature-based in Internet of vehicles," *Advanced Engineering Sciences*, vol. 50, no. 4, pp. 130–134, 2018.

[7] Z. Zhao, *Reserrch on Efficient Group Signatures Schemes in VANET*, Xidian University, Xi'an, China, 2015.

[8] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," *Advances in Cryptology–ASIACRYPT 2003*, Springer, Berlin, Germany, pp. 452–473, 2003.

[9] H. Chen, C. Zhu, and R. Song, "Journal of computer research and development," *Journal of Computer Research and Development*, vol. 47, no. 2, pp. 231–237, 2010.

[10] F. Li, P. Liu, and Z. Zhu, "Certificateless signature and group signature schemes based on bilinear pairings," *Computer Engineering*, vol. 37, no. 24, pp. 18–21, 2011.

[11] J. Yin, *The Research on Certificateless Authenticated Group Key Management in Ad Hoc Network*, Beijing Institute of Technology, Beijing, China, 2016.

[12] X. Zhang, Y. Xu, and J. Cui, "Anonymous authentication protocol based on certificateless signature for vehicular network," *Computer Engineering*, vol. 42, no. 3, pp. 18–28, 2016.

[13] C. Song, M. Zhang, W. Peng, Z. Jia, Z. Liu, and X. Yan, "Research on pairing-free certificateless batch anonymous authentication scheme for VANET," *Journal on Communications*, vol. 38, no. 11, pp. 35–43, 2017.

[14] Y. Chen, X. Cheng, S. Wang, and M. Gao, "Research on certificateless group signature scheme based on bilinear pairings," *Netinfo Security*, vol. 3, pp. 53–58, 2017.

[15] N. Zhao, G. Zhang, and X. Gu, "Certificateless aggregate signature scheme for privacy protection in VANET," *Computer Engineering*, vol. 46, no. 1, pp. 114–128, 2020.

[16] Y. Gan, K. Wang, and L. He, "RFID tag dynamic ownership transfer protocol of multi-owner with TTP weight," *Journal of Light Industry*, vol. 33, no. 1, pp. 72–78, 2018.

[17] Y. Xiao, J. Du, M. Wen, K. Zhou, J. Jiao, and J. Pei, "Traffic sign detection and recognition based on color features and improved support vector machine algorithm," *Journal of Light Industry*, vol. 33, no. 3, pp. 57–65, 2018.