Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7881079, 13 pages
https://doi.org/10.1155/2022/7881079

Research Article

A Novel Identity-Based Mutual Authentication Scheme for Vehicle Ad Hoc Networks

Chaofan Di[1,2] **and Wanqing Wu**[1,2]

[1]*School of Cyber Security and Computer, Hebei University, Baoding, China*
[2]*Key Laboratory of High Trusted Information System in Hebei Province (Hebei University), Baoding, China*

Correspondence should be addressed to Chaofan Di; hbu_dicf@163.com

Received 12 February 2022; Accepted 30 March 2022; Published 19 April 2022

Academic Editor: Daniel G. Reina

The vehicle ad hoc network (VANET) is an emerging industry that deeply integrates a new generation of network communication technology with automotive and road transportation. As the basic nodes of VANETs, vehicles can communicate and share information with other peer vehicles. However, with the rapid development of the industry, the security risks of VANETs, especially the problem of privacy leakage, have become increasingly prominent. To solve this problem, we propose a novel identity-based mutual authentication scheme (IBMA) for vehicle ad hoc networks. In this scheme, we adopt identity-based cryptography (IBC) to generate keys, which reduces the storage burden of the central authority and eliminates the need to rely on the certificate to distribute the public key. Meanwhile, the key escrow issue can be solved, which is a common problem in IBC. Then, the scheme adjusts central authority to semihonest and realizes unconditional privacy protection. In addition, our scheme achieves complete anonymity, which can prevent any other entities such as peer vehicles and central authorities from tracking vehicles. Finally, our scheme provides efficient traceability while protecting vehicle privacy. Security analysis shows that the proposed scheme satisfies a variety of security requirements such as anonymity, reliability, and nonrepudiation. Performance analysis demonstrates that our proposed scheme is efficient and requires less communication and storage cost compared with related schemes.

1. Introduction

In recent years, with the rapid development of wireless communication technology, sensor technology, and mobile computing, vehicular ad hoc network (VANET) [1] has attracted more and more attention from governments, enterprises, and scientific research institutions. VANETs are large-scale mobile self-organizing networks, which are important parts of intelligent transportation systems and autonomous driving. In VANETs, each vehicle is a basic network node that communicates with others to share or exchange data, so that the vehicle can remotely obtain the driving status and road condition information of other vehicles, thereby reducing congestion, avoiding potential traffic accidents, and improving travel efficiency and safety.

The VANET can build a network in the form of self-organization to realize self-configuration and self-management without fixed infrastructure and provide services such as access, data exchange, and resource sharing for each vehicle. Because of its numerous nodes and flexible organization, scholars have envisaged a variety of new services for VANETs, such as dynamic route planning [2] and mobile entertainment in-vehicle [3]. For example, drivers can obtain the latest traffic conditions or parking information through VANETs, and passengers can chat or exchange files through VANET, which greatly improves the travel experience of drivers and passengers.

While providing convenient services for drivers and passengers, VANETs also bring huge security challenges. The security and privacy issues [4] of VANETs have also received increasing attention. Because the VANETs are deployed in the public network area and transmit messages through a wireless network, it is vulnerable to damage by malicious attackers, such as publishing wrong road

condition information and stealing user privacy. The damage directly affects the personal and property security of drivers and passengers. Therefore, the key to comprehensively promoting the VANETs is to solve the problems of information security and privacy protection first.

One of the solutions is to authorize all legal vehicles connected to the network and check whether the vehicles are legal through identity authentication before the communication. Illegal identities will be refused to provide services. At the same time, the privacy of vehicle users should be protected during identity authentication. For example, the real identity of the vehicle should be kept secret during authentication, and location information will not be obtained by authentication agencies [5].

The current research on vehicle ad hoc networks is mainly based on shared key schemes or public key systems [6, 7]. The shared key scheme relies on key management to a large extent, while the traditional public key infrastructure (PKI) puts forward strict requirements for the large-capacity storage and management of public key certificates. In recent years, many authentication schemes using ID-based encryption have been proposed [8–10]. Identity-based encryption (IBC) [11] was first proposed by Shamir in 1984. The basic idea of IBC is that the entity's public key is directly derived from its public identity information (such as phone number and email address), and the private key is calculated and distributed by a central authority. IBC completely eliminates the need for traditional PKI to distribute public keys through certificates. However, in IBC, since the user's private key is completely determined by TA; when the TA is maliciously attacked or the TA itself is not trusted, it will cause an incalculable risk to the system, that is, the key escrow problem [12], which makes it impossible to achieve strong nonrepudiation.

In general, traditional VANETs are composed of three components, namely the trusted authority (TA), the roadside unit (RSU), and the vehicles. TA provides various network services to vehicles through RSUs. The RSUs are fixed on both sides of the roads, which are used to connect the vehicles to the TA. There are also some models without RSU [13], where the vehicle communicates directly with the TA.

In this paper, we propose a novel identity-based mutual authentication scheme for vehicle ad hoc networks. Compared with the existing VANET authentication schemes, our scheme has many advantages:

First, the proposed scheme satisfies various security requirements in the VANET authentication model, such as anonymity, traceability, and nonrepudiation. Meanwhile, it can resist common attacks.

Second, we adopted two independent and parallel trusted authorities to reduce the trust level in TAs. We assume that TA_a and TA_b are well-known cloud platforms (e.g., IBM Cloud and Microsoft Azure) which are supervised by the government and have no incentive to collude to damage their reputation. Two TAs cooperate with each other to generate a pseudonym (PID) corresponding to the real identity (RID) for the vehicle. Therefore, our scheme maintains traceability while ensuring anonymity.

Third, we adopt ID-based encryption to calculate keys, which reduces the storage burden of TA. Besides, we solve the common key escrow problem in the IBC encryption model.

The remainder of the paper is organized as follows. Section 2 summarizes the related work of the previous literature. Section 3 introduces the parameters. The system model, attack model, and specific scheme of the proposed protocol are presented in Section 4. Section 5 analyzes the security of the proposed scheme. In Section 6, performance analysis is done in terms of communication cost, storage cost, and computational cost. Finally, Section 7 concludes the paper and suggests some future directions.

2. Related Work

In this section, we summarize and compare the related work of the previous literature. In recent years, many scholars have researched and explored the problems in the authentication process of vehicle ad hoc networks [14–16].

In terms of the realization of privacy protection and anonymous authentication, the existing solutions can be classified into two main categories: pseudonym-based authentication protocols and group-based authentication protocols.

Pseudonym-based authentication protocols mean that users use pseudonyms to replace their real identities in the process of access authentication or communication. In 2007, Raya and Hubaux [17] proposed a signature-based authentication scheme. In this scheme, when the vehicle wants to sign a message, it first randomly selects a private key from the certificate distributed by the central authority and signs the message with the private key. The receiver verifies whether the identity of the other party is legal by checking the validity of the certificate, thereby completing identity authentication. The disadvantage of this scheme is that the computational cost is high, and the vehicle has to validate for potential revocation when selecting the certificate, which is not suitable for large-scale networks. In 2011, Studer et al. [18] proposed an anonymous authentication scheme based on temporary keys. The scheme signs messages with a short-term key certified by a central authority and provides an efficient revocation method to prevent attackers from obtaining vehicle location and other private information. However, this scheme requires a central authority to maintain the certificate and allows tracking of the current location of vehicles. Therefore, the privacy of vehicles has not been fully protected. Liu et al. [19] proposed a protocol that uses OBU to generate its own anonymous identity and temporary encryption key for identity verification.

In order to further protect the privacy of vehicles, Huang et al. [20] proposed a privacy preservation scheme, namely, the pseudonymous authentication-based conditional privacy. In this scheme, the motor vehicles division (MVD) and roadside units (RSUs) jointly generate pseudonyms for vehicles. MVD generates identification tickets for vehicles, and then, RSU generates pseudonym tickets based on identification tickets. Finally, the vehicle generates its pseudonym based on pseudonym tickets. During the pseudonym

generation process, neither MVD nor RSU knows the true identity of the vehicle. The protocol proposed a revocation method; unfortunately, the calculation overhead of the revocation method is high. Wei et al. [21] proposed a random authentication protocol, which divides the central authority into registration server (RS) and verification server (VS). RS generates pseudonyms by homomorphic encryption. VS is responsible for verifying whether the pseudonyms are legal, which improves system security, and the dependence of the whole system on the central authority is reduced. However, this scheme still has the risk of leaking user privacy, and the computational cost is relatively high.

The concept of group signature was first proposed by Chaum and Heyst [22] in 1991. The basic idea is that the group manager authenticates the vehicles and divides the vehicles into different groups, so that vehicles within and between groups can realize anonymous communication. The communication party can only determine which group the other party belongs to, whether it is a valid group member, and does not know its real identity. When a dispute occurs, the group manager can reveal the suspect vehicle's real identity. Lu et al. [23] proposed a conditional privacy protection protocol for vehicle secure communication. The RSU, as a group manager, dynamically generates a short-term group key between vehicle and RSU, achieving anonymity and traceability. In the meantime, the scheme also alleviates the storage burden of the key. However, the security of this scheme is slightly insufficient. When multiple RSUs are damaged, the scheme cannot provide unlinkability and traceability. In order to solve this problem, Jung et al. [24] proposed a robust conditional privacy protection protocol, which improves the robustness without reducing efficiency. When multiple RSUs are compromised, the scheme can also provide unlinkability and traceability. In addition, the scheme adopts multiple anonymous certificates to reduce the computational overhead of RSU. Zakarya et al. [25] proposed a password-based conditional privacy protection authentication protocol and group key agreement protocol. The scheme provides group key generation, user joining, and leaving functions, and it is lightweight in terms of computing and communication.

Other schemes are aimed at achieving identity authentication that can be roughly divided into the following three categories: public key-based authentication model, identity-based authentication model, and message authentication code- (MAC-) based authentication model. The public key-based authentication model is the traditional public key infrastructure (PKI) model. PKI provides a series of basic services that support public key cryptographic applications (such as encryption and decryption, signature, and verification signature), and its most basic component is the public key certificate. The user's private key is kept secretly by itself, and the user's public key is saved by the certificate which is kept by the central authority. Malik and Pandey [26] proposed a discrete event-based threat-driven authentication scheme. This scheme utilizes asymmetric cryptography, reencrypt key, and time-based arbitrary numbers to provide authentication among vehicles and between vehicles and RSUs. Besides, this scheme also provides privacy protection among vehicles and between vehicles and RSUs, which improves security and can prevent common authentication attacks in VANETs.

The main limitation of PKI is the large storage overhead and the difficulty of certificate management. Shamir first proposed the concept of identity-based encryption (IBC) in 1984. The basic idea of IBC is that the public key of the entity participating in the communication comes directly from its public identity information instead of the traditional random number-like string, and the private key is calculated and distributed by the central authority. IBC completely eliminates the need to implement public key distribution through traditional public key certificates. Li et al. [27] proposed an efficient message authentication with an enhanced privacy scheme based on ring signature and identity-based signature. This scheme achieves unconditional privacy and can resist common attacks such as full key exposure attacks and identity attacks. At the same time, this scheme has a lower computational overhead. Alazzawi et al. [28] proposed an identity-based privacy protection authentication scheme, which can meet the security and privacy requirements and can resist various common attacks. However, the identity-based authentication model has the problem of key escrow, and complete privacy protection can only be achieved when the central authority is fully trusted. Based on this problem, Asari et al. [29] proposed a hierarchical authentication protocol. In this scheme, only part of the private key generated by the authority is used as a partial-private key. The combination of the partial-private key and the random number independently selected by the user is the user's real private key. This means that only legitimate users can obtain the partial-private key, and the key used for communication and signature is only owned by the user, which solves the key escrow problem.

Message authentication code (MAC) is a public function of message and key, and its output is a short block of fixed-length data. Asl and Samavi [30] proposed a symmetric nonrepudiation message authentication scheme. This scheme combines symmetric key encryption and digital signature, allowing RSU to verify the authenticity of the information sent by the vehicle, and achieves nonrepudiation. The weakness is that the message verification process relies too much on the RSU. Pandi et al. [31] proposed a dual authentication method based on a hash code. This method uses a hash code (HC) to generate an authentication code (AC) for authentication. However, in this method, the user's pseudonym is randomly generated and has no calculation relationship with the real identity. Therefore, there is a risk of excessive storage burden and vulnerability to leakage. Benyamina et al. [32] proposed an efficient and lightweight authentication scheme for vehicular ad hoc networks. This scheme adopts MAC functions and XOR operations to sign and verify messages. On the premise of ensuring security and privacy protection, the scheme reduces the computation and communication costs. However, this scheme still has the disadvantage of key escrow and high storage overhead.

In addition, there are protocols based on XOR operations [33], which are very fast in the calculation, but they are not sufficiently secure.

Compared with most of the existing authentication schemes in the literature, this paper proposes a novel

identity-based mutual authentication scheme, which is aimed at strengthening the protection of vehicle user privacy during authentication. In our scheme, the authentication of the vehicle and the TA is two-way, that is, the TA needs to verify the legitimacy of the vehicle's identity, and the vehicle can also verify the legitimacy of the TA. In addition, we lowered the TA's trust level and divided the TA into two parts. One receives the real identity information of the vehicle, and the other generates pseudonyms. We also adopt IBC to reduce the storage overhead of TA and solve the key escrow problem in IBC by generating communication keys by the vehicles themselves. Finally, our solution achieves efficient traceability while protecting vehicle privacy.

3. Preliminaries

For a better understanding, we first briefly introduce the basic knowledge required for the article.

3.1. Bilinear Pairings. Let G_1 be an additive group and G_2 be a multiplicative group of the order q. Let P be an arbitrary generator of G_1. A bilinear pairing can be defined if the mapping $e : G_1 \times G_1 \longrightarrow G_2$ satisfies the following properties:

(i) Bilinear: for $\forall P, Q \in G_1$ and $a, b \in Z_q^*$

$$e(aP, bQ) = e(P, Q)^{ab} \quad (1)$$

(ii) Nondegenerate: $\forall P, Q \in G_1, e(aP, bQ) \neq I_{G_2}$, where I_{G_2} is an arbitrary generator of G_2

(iii) Computable: for $\forall P, Q \in G_1$, there exists a polynomial time algorithm to compute $e(P, Q)$

3.2. Security Assumptions. In this section, we define the following security assumptions, which are assumed to be difficult to break by any polynomial time-bounded algorithm.

3.2.1. Definition 1 (Large Integer Factoring Problem (IFP))

(1) Given two prime numbers p and q, and it is easy to calculate $n = p \times q$

(2) Given an integer n, it is difficult to find the prime factors p and q of n satisfying $n = p \times q$

3.2.2. Definition 2 (Elliptic Curve Discrete Logarithm Problem (ECDLP)). Given a random instance $<P, Q>$, where $P \in G_1$, $Q \in G_1$, it is hard to find x satisfying $Q = xP$.

3.3. Notations and Explanations. The relevant notations and explanations used in our scheme are shown in Table 1.

Table 1: The notations and explanations.

Nations	Explanations
TA_a	Trusted authority a
TA_b	Trusted authority b
V	Vehicle
G_1, L_1	Additive groups
G_2, L_2	Multiplicative groups
P_a, P_b	Arbitrary generators of the additive group G_1, L_1
q_a, q_b	Orders of the multiplicative group G_2, L_2
pk_a, sk_a	Public and private key pair of TA_a
pk_b, sk_b	Public and private key pair of TA_a
e	Bilinear pair
H_a, H_b	Hash functions
RID	Real identifier
PID	Pseudo identifier
$A \longrightarrow B\{M\}$	Entity A sends M to entity B
$E^1()$	Public key encryption
$E^2()$	Symmetric encryption
r, k_1, k_1	Random numbers
Q_V, S_V	IBC public and private key pair of vehicle V
x, y	RSA public and private key pair of vehicle V
T	Valid time
T_0, T_1, T_2	Current timestamp
a, b	Large prime numbers
c	Ciphertext
m	Communication message
K	Session key

4. Authentication Protocol

4.1. Overview of the Protocol. Vehicles TA_a and TA_b are the three components in our proposed system. It consists of a hierarchy of two layers where the vehicles are in lower layer, and TA_a and TA_b are in a higher layer. Vehicles are the entities that would like to communicate with other peer vehicles via VANETs. Two different authorities are deployed, which are denoted as TA_a and TA_b, respectively. In our proposed protocol, the TA_a and TA_b act as a high computational entity with large storage capacity but they are not absolutely trusted. The two authorities collaborate with each other to ensure privacy-preserving vehicle authentications. If one of them was compromised, none of them would be able to track the vehicle alone.

4.2. Threat Model. In our scheme, we adopt the following threat or adversary model.

(i) We assume that the two trusted authorities used in our authentication system are semihonest. In other words, they follow the prescriptive procedures of the proposed protocol and do not collude with each other

(ii) Vehicles in VANETs may be malicious. Malicious vehicles may impersonate other vehicles to communicate with other peer vehicles

(iii) We assume that the communication channel is insecure, which means that a powerful attacker can eavesdrop and capture communication information.

Besides, we consider a situation that adversaries with high computing power may reveal sensitive information by violent attacks or other methods (such as replay attack [34])

4.3. The Proposed Protocol. In this section, we explain the secure authentication scheme for VANETs. The system of the proposed scheme is composed of two independent and parallel trusted authorities TA_a, TA_b, and vehicle V, aiming at achieving secure authentication communication in vehicle ad hoc networks. We assume that the time of all entities in the system is synchronized and the communication between TA_a and TA_b uses a secure and fast dedicated channel. The proposed authentication protocol is divided into five parts: initialization, vehicle registration, V2V communication, vehicle tracing, and revocation.

4.3.1. Initialization. The initialization phase is the process of generating system parameters of the vehicle ad hoc network. The details are as follows:

(i) TA_a: define G_1 to be an additive group and G_2 to be a multiplicative group with $|G_2| = q_a$. P_a is an arbitrary generator of G_1. Let H_a be a cryptography hash function where $H_a : \{0,1\}^* \times G_1 \longrightarrow Z_{q_a}^*$. TA_a chooses a private key $sk_a \in Z_{q_a}^*$ randomly and computes a corresponding public key:

$$pk_a = \left(\underbrace{P_a + P_a + \cdots + P_a}_{sk_a} \right) = sk_a \times P_a. \tag{2}$$

Note that pk_a is calculated from the private key sk_a, but according to Definition 2, even if the attacker obtains P_a and pk_a, it is hard to find sk_a satisfying $pk_a = sk_a \times P_a$.

Then TA_a publishes pk_a and keeps the private key sk_a secret. Then the public system parameters of TA_a are $<G_1, G_2, pk_a, P_a, q_a, H_a>$

(ii) TA_b: define L_1 to be an additive group and L_2 to be a multiplicative group with $|L_2| = q_b$. P_b is an arbitrary generator of L_1. The pairing $e : L_1 \times L_1 \longrightarrow L_2$. Let H_b be a cryptography hash function where $H_b : \{0,1\}^* \times L_1 \longrightarrow Z_{q_b}^*$. TA_b chooses a private key $sk_b \in Z_{q_b}^*$ randomly and computes a corresponding public key:

$$pk_b = \left(\underbrace{P_b + P_b + \cdots + P_b}_{sk_b} \right) = sk_b \times P_b. \tag{3}$$

Then TA_b publishes pk_b and keeps the private key sk_b secret. Then the public system parameters of TA_b are $<L_1, L_2, pk_b, P_b, q_b, H_b, e>$.

4.3.2. Vehicle Registration. The vehicle registration phase is the process in which the vehicle is authenticated by two trusted authorities and obtains a pseudo identifier (PID) and private key. The registration model is shown in Figure 1. The registration phase is performed as follows:

(1) The vehicle V encrypts its real identifier (RID) with TA_a's public key pk_a and uses pk_b to encrypt a random number r which is selected by itself. Then, two ciphertexts are sent together to TA_a, summarized as

$$V \longrightarrow TA_a : \left\{ E^1_{pk_a}(RID), E^1_{pk_b}(r) \right\}, \tag{4}$$

where $E^1()$ is the public key encryption algorithm.

(2) After receiving $\{E^1_{pk_a}(RID), E^1_{pk_b}(r)\}$, TA_a decrypts $E^1_{pk_a}(RID)$ with its private key sk_a to obtain RID. Then TA_a executes the following calculations:

$$PID' = RID \oplus H_a(sk_a), \tag{5}$$

where $\oplus$ denotes as bitwise XOR operations.

After obtaining PID′, TA_a deletes RID and sends PID′ to TA_b together with $E^1_{pkb}(r)$ received previously. Since a secure and fast dedicated channel is used between TA_a and TA_b, the PID′ does not need to be encrypted. That is

$$TA_a \longrightarrow TA_b : \left\{ PID', E^1_{pkb}(r) \right\} \tag{6}$$

(3) TA_b gets PID′ and uses its private key sk_b to decrypt the received message to learn r and then calculates

$$PID = PID' \oplus H_b\left(sk_b \| T \| T' \right), \tag{7}$$

$$S_V = sk_b \times H_b(PID), \tag{8}$$

$$Q_V = H_b(PID). \tag{9}$$

PID is the pseudonym of the vehicle for subsequent communication. T is the valid time of PID, and T' denotes the generation time of PID. If a vehicle's pseudonym expires, TA_b can regenerate its pseudonym based on the current time. S_V and Q_V are private key and the corresponding public key of the vehicle V, respectively.

It is worth noting that in order to reduce the vehicle's calculation burden, Q_V is calculated by TA_b. TA_b takes the random number r as the key of symmetric encryption, encrypts PID, S_V, and Q_V with r, and sends the ciphertext to TA_a. Meanwhile, TA_b stores the PID, T, and T' in the database. In the pseudonym generation process, TA_a saves the real identifier RID, and TA_b saves the pseudo identifier

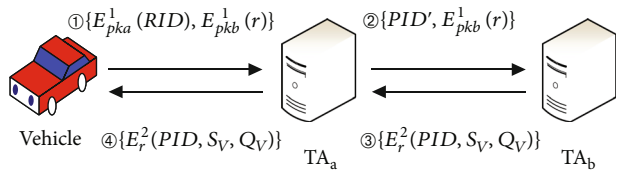

Figure 1: Registration model.

(PID). The sending process can be expressed as

$$\mathrm{TA}_b \longrightarrow \mathrm{TA}_a : \left\{E_r^2(\mathrm{PID}, S_V, Q_V)\right\}, \tag{10}$$

where $E^2()$ is the symmetric encryption algorithm.

(4) After receiving $E_r^2(PID, S_V, Q_V)$, TA_a will forward it to vehicle V without any processing, denoted as

$$\mathrm{TA}_a \longrightarrow V : \left\{E_r^2(PID, S_V, Q_V)\right\} \tag{11}$$

(5) V decrypts $E_r^2(PID, S_V, Q_V)$ with a random number r to obtain PID, S_V, and Q_V when receiving the ciphertext. Then V checks $e(S_V, P_b) = ?e(Q_V, pk_b)$. If the equation holds, it can prove that the received message is from a valid TA_a. After the verification, vehicle V randomly selects two large prime numbers a and b and calculates

$$n = a \times b, \tag{12}$$

$$\varphi(n) = (a-1) \times (b-1), \tag{13}$$

$$y = Q_V \times P_b. \tag{14}$$

Note that y and $\varphi(n)$ should satisfy $1 < y < \varphi(n)$ and $(e, \varphi(n)) = 1$; otherwise, V should reselect a and b. If the constraint is met, V computes x in terms of $xy = 1 \bmod \varphi(n)$.

x and y are the private key and public key of vehicle V for subsequent communication, respectively, and the private key x is only owned by vehicle V, thus avoiding the problem of key escrow.

4.3.3. V2V Communication. Vehicle-to-vehicle (V2V) communication phase is the process in which vehicle V_1 and other peer vehicle V_2 complete authentication to each other and generate session key with the participation of the trusted authority TA_b. Figure 2 shows the communication model. A detailed description is as follows:

(1) V_1 searches for the intended vehicle V_2 and obtains V_2's pseudonym PID_2.(We can search for the intended vehicle based on the deep neural network [35]. The search process is not the focus of this paper, so the detailed search process will not be described here. Then V_1 encrypts the pseudonym and current time T_0 with TA_b's public key pk_b and

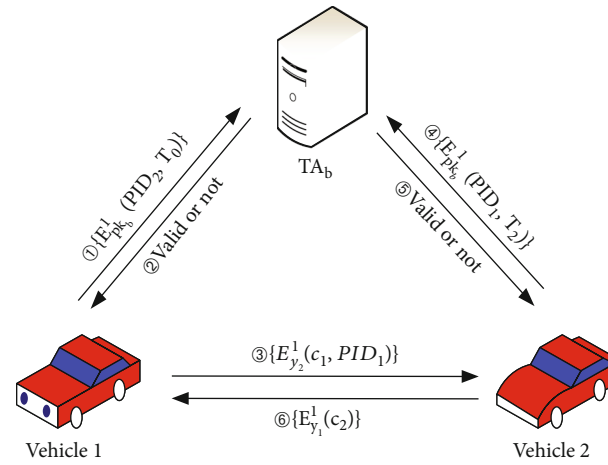

Figure 2: Communication model.

finally sends it to TA_b to determine whether the pseudonym is legal or not. That is to say

$$\mathrm{V}_1 \longrightarrow \mathrm{TA}_b : \left\{\mathrm{E}_{pk_b}^1 (PID_2, T_0)\right\} \tag{15}$$

(2) TA_b searches for PID_2 in the local database after receiving the message and obtaining PID_2, T_0. If there is a matching PID_2 and it is within the validity time, TA_b returns the valid message of pseudoidentifier to V_1. Otherwise, an invalid message of pseudoidentifier is returned. Note that if PID_2 is a timed-out pseudonym, it is necessary to delete the pseudonym in the database while returning a pseudonym invalid message

(3) V_1 believes that V_2 is a legal vehicle and then calculates ciphertext c_1 and V_2's public key y_2:

$$c_1 = E_{x_1}^1(m_1 \| T_1 \| k_1), \tag{16}$$

$$y_2 = \mathrm{Q}_{V_2} \times \mathrm{P}_b = \mathrm{H}_b(PID_2) * \mathrm{P}_b. \tag{17}$$

where m_1 means the communication message, T_1 is the current time, and k_1 denotes the random number selected by the vehicle V_1. When the calculation is completed, V_1 sends ciphertext c_1 and its own pseudoidentifier PID_1 to V_2, both of which are encrypted with V_2's public key pk_b. That is

$$\mathrm{V}_1 \longrightarrow \mathrm{V}_2 : \left\{\mathrm{E}_{y_2}^1 (c_1, PID_1)\right\} \tag{18}$$

(4) Upon receiving the message, V_2 decrypts the message with its own private key x_2 to obtain c_1 and PID_1. Then V_2 encrypts PID_1 and current time T_2

with TA_b's public key pk_b. Finally V_2 sends the ciphertext to TA_b for verification. That is

$$V_2 \longrightarrow TA_b : \left\{E^1_{pk_b}(PID_1, T_2)\right\} \tag{19}$$

(5) After getting PID_1 and T_2, TA_b checks whether PID_1 exists in the local database and verifies whether it has expired. If it is legal and valid, TA_b returns the valid message of pseudoidentifier to V_2. Otherwise, an invalid message pseudoidentifier is returned. (Similarly, if PID_1 is a timed-out pseudonym, it should be deleted from the local database while returning a pseudonym invalid message)

(6) After V_2 confirms that V_1 is legitimate, V_2 calculates V_1's public key y_1 and decrypts the ciphertext c_1 to obtain m_1, T_1, and k_1

First, check whether the timestamp T_1 is fresh or not. If T_1 is fresh, V_2 computes

$$c_2 = E^1_{x_2}(m_2 \| T_3 \| k_2), \tag{20}$$

$$K = k_1 \oplus k_2, \tag{21}$$

where m_2 denotes the communication message, T_3 is the current time, and k_2 means the random number selected by the vehicle V_2. K is the session key for subsequent communication. Then V_2 encrypts ciphertext c_2 with V_1's public key pk_1 and sends the cyphertext to V_1. That is

$$V_2 \longrightarrow V_1 : \left\{E^1_{y_1}(c_2)\right\} \tag{22}$$

(7) After receiving the message, V_1 decrypts the ciphertext c_2 and obtains m_2, T_3, and k_2. If T_3 is fresh, V_1 calculates the session key $K = k_1 \oplus k_2$ for subsequent communication with V_2. Otherwise, V_2 rejects the messages

4.3.4. Vehicle Tracing. In practical application, disputes may occur from time to time due to various reasons. Sometimes, third-party law enforcement agencies may want to know the real identity of the malicious vehicle immediately. The vehicle tracking phase is a process in which TA_a and TA_b cooperate with each other and track the suspect vehicle's real identifier according to its pseudonym. The tracing model is depicted in Figure 3. And the detailed process is as follows:

(1) After receiving malicious vehicles' PID from law enforcement agencies, TA_b searches the corresponding T, T', and computes

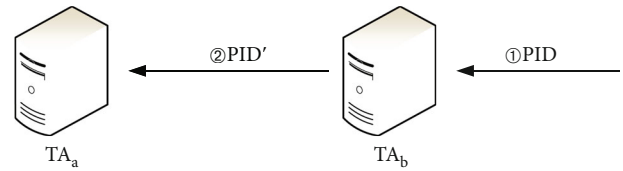

Figure 3: Tracing model.

$$PID' = PID \oplus H_b\left(sk_b \| T \| T'\right) \tag{23}$$

and sends the encrypted PID' to TA_a:

$$TA_b \longrightarrow TA_a : \left\{PID'\right\} \tag{24}$$

(2) TA_a extracts RID from the receiving PID':

$$RID = PID' \oplus H_a(sk_a) \tag{25}$$

Therefore, the real identity is successfully tracked.

4.3.5. Vehicle Revocation. In the revocation phase, when the vehicle is confirmed as a malicious vehicle, or the validity period of its pseudonym expires, the central authority shall remove it from the system in time. When TA_b gets the pseudoidentifier of the vehicle to be removed, pseudonym information will be deleted from the local database. After that, the authentication request on this pseudonym will fail, because there is no matching legal pseudonym in TA_b's database.

5. Security Analysis

In this section, we will show that the proposed scheme is correct and secure with respect to the assumption in Section 3.2.

5.1. Formal Security Analysis

Theorem 1. *The proposed mutual authentication protocol IBMA is secure assuming that (a) the large integer factoring problem (IFP) is computationally hard and (b) the elliptic curve discrete logarithm problem (ECDLP) is difficult to break by any polynomial time-bounded algorithm.*

Proof. We start examining the security of the vehicle's private and public key, x and y, respectively. For every probabilistic polynomial time adversary A, there is a negligible ϵ such that

$$\Pr\left[A(n) \in \{a, b\}\right] \leq \epsilon(l), \tag{26}$$

where a and b are primes with size l bits and $n = a \times b$.

a and b are two large prime numbers selected by the vehicle. In order to ensure the security, n should be 2048 bits, which is generally used in RSA [36], and the size of a

and b should be 1024 bits. There are approximately 2^{1015} prime numbers of size less than 1024 bits according to [37], which makes it computationally hard for an adversary to find a or b.

Based on [38], the most famous heuristic asymptotic running time algorithm of prime number factorization runs on average in time $2^{O(l^{1/3}\cdot(\log l)^{2/3})}$ to factor a number of size l bits. Therefore, $\epsilon(l) = 1/2^{O(l^{1/3}\cdot(\log l)^{2/3})}$. The above analysis shows that n is secure in our protocol. The same logic as for n works to show that $\varphi(n)(\varphi(n) = (a-1)\times(b-1))$ is also secure. □

The above implies the security of Theorem 1 (a) and proves that the generation of vehicles' RSA private and public keys is secure.

In the proposed protocol, the generation of some public keys (e.g., pk_a, pk_b) is computed and deduced from the private key. The security of these public and private key pairs is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). At present, the best-known algorithm for solving the elliptic curve discrete logarithm problem is the distributed $Pollard-\rho$ method [39], and the computational complexity is $O((\pi n/2)^{1/2}/m)$, where n is the largest prime factor of the order of the group and m denotes the number of CPUs used by the distributed algorithm. It can be seen that the elliptic curve cryptography is safe when the prime numbers q and n are large enough. This is the fundamental reason that the order of the elliptic curve solution point group must have a large prime factor. In an ideal situation, the order of the group itself is a large prime number.

For common security assumptions (e.g., large integer factorization and discrete logarithm problems), there are algorithms with subexponential complexity for the time being [40], but there is no subexponential algorithm for solving the intended vehicle elliptic curve discrete logarithm problem. Therefore, ECDLP is difficult to break by any polynomial time-bounded algorithm.

The above complexity analysis shows the difficulty of ECDLP and proves the security of public key generation in our protocol.

5.2. Correctness. The proposed scheme is correct and consistent because of the following reasons:

In the registration phase, the vehicle V first sends its real identity RID and random number r to TA_a, where RID and r are encrypted with pk_a and pk_b, respectively. Thus, the transmission of RID and r is safe. Attackers cannot reveal RID and r without knowing sk_a and sk_b. After receiving RID, TA_a calculates PID' and then sends PID' and the received ciphertext about r to TA_b. Note that in order to further strengthen security, TA_a will not store RID but removes it after calculating PID' to avoid leakage. TA_b calculates PID according to the received PID' and then computes the public and private key pair Q_V and S_V of the vehicle. Finally, TA_b sends PID, S_V, and Q_V to TA_a. Since r was encrypted with pk_b, TA_a cannot learn the value of random number r. Therefore, PID, S_V, and Q_V are secret. All TA_a can do is to forward the message to the vehicle V.

On receiving $<PID, S_V, Q_V>$, vehicle V computes

$$e(S_V, P_b) = e(sk_b \times Q_V, P_b) = e(Q_V, sk_b \times P_b) = e(Q_V, pk_b). \tag{27}$$

Because the private key sk_b is only held by TA_b, no one else can generate the correct public and private key pair Q_V and S_V that satisfies the equation. In other words, the vehicle can verify whether the TA_b sent $<PID, S_V, Q_V>$ is a legal TA_b according to the equation, thereby verifying the identity of the TA_b, realizing mutual authentication.

In the V2V communication phase, the vehicle V_1 first asks TA_b whether the assumed communication vehicle V_1 's pseudonym is legal. After receiving a positive reply, V_1 generates ciphertext c_1 with its own private key x. After that, V_1 sends c_1 and its own pseudonym PID_1 to the assumed communication vehicle V_2.

Upon receiving the message, V_1 enquires TA_b whether PID_1 is a legal pseudoidentifier. If PID_1 is legal, V_2 calculates the public key y_1 of PID_1 to verify ciphertext c_1; otherwise, it drops the message.

V_2 obtains the communication message m, the timestamp T_1, and the random number k_1 after c_1 is successfully decrypted. Note that if the timestamp is not fresh, the message will also be dropped. Then, V_2 generates ciphertext c_2, which will be sent to V_1 together with its pseudonym PID_2 . V_1 verifies the identity of V_2 in the same way. After the identity verification is passed, the session key is calculated $K = k_1 \oplus k_2$. k_1 is part of the ciphertext c_1. Similarly, k_2 is part of the ciphertext c_2.

If the attacker does not have the key x, it can not generate valid ciphertexts. The vehicle's public and private key pair x and y are based on the difficulty of factorization of large complex numbers, so no attackers can calculate the private key according to the public key in probabilistic polynomial time. In addition, the ciphertext and pseudonym are protected by the receiver's public key. No one else can get the ciphertext and pseudonym.

5.3. Mutual Authentication. The proposed protocol can realize mutual authentication between vehicles and TA_b. TA_b uses PID' sent by TA_a to generate pseudonyms PID and public-private key pair Q_V, S_V for vehicles. Vehicles use the public-private key pair sent by TA_b to verify TA_b. If the public-private key pair Q_V, S_V are not sent by a legal TA_b, the equation $e(S_V, P_b) = ?e(Q_V, pk_b)$ will not hold. In conclusion, TA_b verifies whether vehicle V has submitted its real identity through PID', and vehicle V judges whether TA is legal by equation $e(S_V, P_b) = ?e(Q_V, pk_b)$. Thus, the mutual authentication between vehicles and TA_b is achieved.

The mutual authentication between vehicles is also achieved. Before V2V communicates, vehicle V_1 needs to enquire TA_b whether the pseudonym of the communication vehicle V_2 is legal. Similarly, V_2 confirms the legitimacy of V_1 in the same way. Both the receiver vehicle and the sender vehicle need to confirm that the identity of the other party is

legal before carrying out subsequent communication to avoid being attacked by attackers. Therefore, the proposed protocol realizes mutual authentication.

5.4. Reliability. In the registration phase, when the real identity (RID) is submitted by the vehicle, the communication contents are protected by TA_a's public key. Since the public-private key pair of TA_a is secured based on the ECDLP assumption, no adversary can calculate the private key according to the public key in probabilistic polynomial time. Thus, the information submitted by the vehicle will not be stolen. In addition, PID, S_V, and Q_V sent by TA_b are encrypted by random number r, which is generated by the vehicle and discarded after being used once. No attacker including TA_a can crack it within the effective time. So the registration phase is reliable.

In the V2V communication phase, the message is protected by the public-private key pair x and y of the vehicle, and x and y are generated by RSA, which is based on the difficulty of factorization of a large complex number. No attackers can crack the private key x according to the public key y. Both ciphertexts and pseudonyms are well protected. Besides, the session key K is generated by random numbers generated by both communication parties. The random numbers are in the ciphertexts of the sending vehicles, and the ciphertexts are encrypted by the public key of the receiving parties. No attackers can obtain the random numbers. In conclusion, the V2V communication stage is reliable.

5.5. Anonymity. During the communication, vehicle always uses pseudonym as its identity. The entity communicating with it can only judge whether the pseudonym is legal but cannot know its real identity. The real identity (RID) of the vehicle will no longer appear in the communication contents after it is submitted to TA_a in the registration phase. TA_a will remove RID in time to prevent leakage. TA_b calculates PID according to PID$'$ sent from TA_a. PID is used as communication pseudonym of registered vehicles. No one knows the correspondence between pseudonyms and real names, including TA_a and TA_b. If a vehicle's pseudonym expires, TA_b can regenerate its pseudonym based on the current time.

In the existing schemes, most of them store the corresponding relationship between PID and RID by a single TA, which has potential safety hazards. Once the TA is compromised, or information leakage occurs in the TA, incalculable hazards will happen. In the proposed scheme, two TAs are in charge of the corresponding relationship. If it is needed to recover the real identifier, two TAs must cooperate with each other. Moreover, there is no information about the real identifier in TA's database. Even if the information is leaked, the damage is minimal, which greatly improves the security. Therefore, communication anonymity is realized.

5.6. Unforgeability. Unforgeability aims that only the intended vehicles can make valid ciphertexts and authentication messages. Attackers cannot forge valid ciphertexts and authentication messages generated by legitimate vehicles.

In the vehicle and TA_a authentication phase, the vehicle must submit its real identity in order to obtain a pseudo identifier and become a legitimate vehicle.

In the V2V authentication, the vehicle must be able to generate a valid ciphertext c. At the same time, its pseudonym should exist in the database. If an attacker wants to impersonate vehicle V for communication, he can easily obtain the pseudonym of the vehicle V, because the pseudonym is public. However, he cannot generate a legal ciphertext to pass the verification. Since the private key x is generated by the vehicle itself based on the RSA algorithm, it is not feasible to calculate the private key x according to the public key y. Therefore, the ciphertext c is unforgeable.

5.7. Traceability. Traceability means that TA_a and TA_b have the ability to reveal the real identity of a vehicle in VANETs when it is confirmed as a malicious vehicle.

At first, TA_b obtains the PID of malicious vehicle and calculates the corresponding PID$'$, where $\mathrm{PID}' = \mathrm{PID} \oplus H_b(sk_b \| T \| T')$, and then sends PID$'$ to TA_a. TA_a will recover the real identifier RID, where $\mathrm{RID} = \mathrm{PID}' \oplus H_a(sk_a)$. Both TA_a and TA_b do not know the corresponding relationship between PID and RID. Only when they cooperate with each other can they recover vehicle's real identity. If an attacker wants to capture the real identity corresponding to a pseudonym illegally, he needs to crack the private keys of TA_a and TA_b at the same time. Since sk_a and sk_b are random numbers in $Z^*_{q_a}$ and $Z^*_{q_b}$, respectively, it is almost impossible to crack them at the same time. Thus, traceability is achieved while improving security.

5.8. Nonrepudiation. Nonrepudiation aims that after TA_a traces the real identity of a malicious vehicle, the vehicle cannot deny that it has generate the ciphertext. There is no key escrow problem in the proposed protocol, and the private key x in V2V communication is generated by the vehicle itself. No attacker can calculate x based on the public key y . Therefore, even if TA_a and TA_b are semihonest, the private key x of the vehicle is only owned by itself, and no one else can obtain the private key x to make a legal ciphertext. In conclusion, the scheme is undeniable.

5.9. Related Attack

5.9.1. Replay Attack. A replay attack refers to that a malicious attacker reinjects previously received messages into the VANETs to achieve the purpose of attacking legitimate vehicles. In order to prevent the proposed scheme from replay attacks, we add a timestamp to ciphertexts. The ciphertext can only be made by the sender's vehicle. No one else can forge a legal ciphertext, nor can it change the content of the ciphertext. This is because the attacker cannot obtain the sender's private key. The receiving vehicle can decide whether to accept the message according to the freshness of the timestamp, and the replayed message cannot pass the verification. Therefore, the proposed scheme can effectively prevent the replay attacks.

5.9.2. Man-in-the-Middle Attack. In addition to replay attacks, the man-in-the-middle attack is also a common attack method used by attackers. Because VANETs use wireless public channel communication, they cannot completely resist attackers from eavesdropping on data packets. But all communication contents in our scheme are protected by key encryption.

In the registration phase, during the submission of the real identity, the contents of the communication are protected by the public keys of TA_a and TA_b, and attackers cannot obtain meaningful data even if the message is eavesdropped. In the process of pseudonym and public and private key distribution, the communication contents are encrypted and protected by random number r as a symmetric key. The random number r is generated by the vehicle and discarded after one use. Even if an attacker steals the ciphertext, he cannot infer and modify the content of the plaintext. Therefore, the registration phase can resist the man-in-the-middle attack.

In the V2V communication stage, the communication contents are protected by the public key of the receiver vehicle, and the private key of the vehicle is only owned by himself. Even TA_a and TA_b cannot know the content of the communication. If an attacker wants to crack the ciphertext, it needs to crack the RSA algorithm within a probabilistic polynomial time, which is impossible. Therefore, the communication phase can resist the man-in-the-middle attack. The security comparison is summarized in Table 2.

6. Performance Analysis

In this section, the performance of the proposed protocol will be briefly described. The proposed protocol adopts IBC and RSA encryption. IBC can greatly reduce the amount of computation and save the storage cost, considering that RSA decryption time is relatively long. The hardware decryption method based on the Montgomery algorithm [41] can help to improve the efficiency. Therefore, our protocol is efficient and does not require the vehicle to have high-performance computing equipment. We evaluate the efficiency of the whole authentication process according to communication cost, storage cost, and computational cost. The experimental environment is Intel (R) Core(TM) i7-8700 CPU @ 3.20 GHz, 8 GB RAM with 64-bit Windows 10 operating system.

6.1. Communication and Storage Cost. Communication cost refers to the number of bits of content transmitted in the channel, and storage cost is the cost of storing different parameters in the memory of each entity. The proposed scheme adopts IBC encryption technology, which eliminates the difficulty of traditional PKI key storage, and only needs to save a few parameters, greatly reducing the storage overhead compared with the existing schemes. For TA, the storage cost of TA_a only needs to store its private key secretly except for the public parameters, and there is almost no storage overhead. For TA_b, the user's pseudonym, pseudonym generation time, and valid time need to be stored in addition to the public parameter and private key. The storage overhead is directly proportional to the number of registered vehicles. For vehicles, in addition to the two public and private key pairs and their own pseudonyms, no additional data needs to be saved, and it does not change with the number of vehicles in the network.

In different protocols, the authors used various variables. Generally speaking, the timestamp (C_{TS}) excepts 8 bytes, the real identifier (C_{RID}) requires 10 bytes, the pseudonym (C_{PID}) requires 10 bytes, the multiplication (C_{mul}) requires 10 bytes, the symmetric encryption/decryption (C_{SE}, C_{SD}) takes 16 bytes, the random number (C_R) requires 16 bytes, the hash function (C_h) requires 32 bytes, and the communication message (C_M) 100 bytes are required; 128 bytes are required for public key encryption and decryption (C_{PE}, C_{PD}), 128 bytes are required for homomorphic encryption and decryption (C_{HE}, C_{HD}), and 128 bytes are required for modular exponentiation (C_{ME}); signature algorithm 1 (C_{SIG_1}) requires 42 bytes, signature algorithm 2 (C_{SIG_2}) requires 192 bytes, vehicle information (C_{info}) requires 100 bytes, and communication message (C_M) requires 100 bytes. Besides, n denotes the number of vehicles. The communication and storage overhead are shown in Table 3.

6.2. Computational Cost. The computational cost refers to the time required for cryptographic operations in the phases of pseudonym generation, public-private key pair generation, identity tracking, etc. Four aspects are mainly involved in the registration phase: pseudonym generation, identity-based public and private key pair generation, bilinear pair verification calculation, and RSA public and private key generation. The pseudonym generation includes two XOR operations and two hash operations. Public and private key generation includes a multiplication operation and a hash operation. When verifying the legality of the TA, a bilinear calculation is performed. The calculation of the bilinear calculation is complicated, but compared with other existing solutions, the verification process of the TA by the vehicle is provided; thus, the mutual authentication is realized, and the security in the registration phase is significantly improved. RSA decryption takes a long time, but fortunately, there are many ways to improve the efficiency of RSA decryption, such as hardware decryption.

In the V2V communication phase, in addition to the necessary communication encryption and ciphertext calculation, each vehicle needs to calculate the public key y of the vehicle communicating with it. The process of calculating the public key y includes a hash operation and a multiplication operation. Although the amount of calculation has been slightly increased, the difficulty of storing traditional PKI public key certificates is eliminated. Now, TA_b only needs to store the pseudonym and its validity time locally, and other required content can be calculated based on public parameters, reducing the storage cost of TA. Moreover, the vehicle has to calculate the session key, which requires only one XOR operation.

In the tracing phase, TA_a and TA_b only need to perform a hash operation and an exclusive XOR operation, respectively.

Table 2: Security comparison.

Scheme	Replay attack	Man-in-the-middle attack	Anonymity	Forgery attack	Traceability	Nonrepudiation	Key escrow
GISI [6]	√	√	√	√	√	×	×
ACPN [7]	√	×	√	√	√	√	×
PPDAS [19]	√	√	√	√	√	×	×
VGKM [31]	√	√	√	√	√	×	×
RA [21]	√	√	√	√	√	×	×
ANEL [32]	√	√	√	√	√	√	×
P^2-SHARP [33]	√	√	√	×	√	×	/
Our scheme	√	√	√	√	√	√	√

Table 3: Communication and storage cost.

Scheme	Communication cost	Storage cost
GSIS [6]	C_{SIG_2}	$5C_{RID} + 4C_{TS} + 2C_M + C_{SIG_1} + C_{SIG_2}$
ACPN [7]	$10C_{RID} + 7C_{TS} + 7C_{PE} + 4C_M + 7C_{SIG_1}$	$5C_{PE} + 5C_{PD}$
PPDAS [19]	$3C_{RID} + 6C_{TS} + 17C_h + 6C_{PE} + 4C_{mul} + 3C_M$	$5C_{RID} + C_{TS} + 7C_h$
VGKM [31]	$6C_{PE} + C_{RID} + C_{PID} + C_{TS} + C_{SIG_2}$	$3C_R + 2C_{RID}$
RA [21]	$C_{RID} + 5C_{PID} + 2C_R + 3C_{HE}$	$2C_{PID} + 2C_R + nC_{RID}$
ANEL [32]	$C_{info} + 7C_R + 2C_{PID} + 2C_{RID} + C_M + C_h + C_{TS}$	$2C_{PID} + C_{RID} + 4C_h + 7C_R + 2C_{TS}$
P^2-SHARP [33]-LWN	$3C_{RID} + 4C_{TS} + 8C_h$	$5C_{RID} + 2C_h$
P^2-SHARP [33]-GWN	$C_{RID} + 2C_{TS} + 6C_h$	$5C_{RID} + 2C_h$
Our scheme	$C_{PID} + 3C_{PE} + 2C_{SE}$	$4C_R + 2C_{PID} + 2C_{TS}$

Different authors use a variety of operations in their protocols. According to our simulation results, it is measured as follows: one-way hash function operation time: $T_h = 0.0020$ ms; public key encryption and decryption time: $T_{PE} = 4.4063$ ms; $T_{PD} = 7.7613$ ms; symmetric encryption and decryption time: $T_{SE} = 4.4063$ ms, $T_{SD} = 7.7613$ ms; homomorphic encryption and decryption time: $T_{HE} = 1.879$ ms, $T_{HD} = 1.879$ ms; signature time and verification signature time: T_{SIG}=24.8351 ms, T_{SIGV}=1.8235 ms, multiplication, division, and addition operation time: $T_{mul} = 0.0268$ ms, $T_{\text{div}} = 0.0012$ ms, and $T_{add} = 0.0017$ ms; MAC calculation time: $T_{MAC} = 0.0097$ ms; bilinear pairing calculation time: $T_{BP} = 4.2100$ ms; and exponential operation time: $T_E = 0.0399$ ms. Compared with other operations, the time of XOR operation is negligible.

It is worth noting that our scheme adopts multiple cryptographic techniques such as public key encryption, symmetric encryption, and bilinear pairing to improve security. As a result, the proposed scheme realizes multiple requirements that cannot be met by existing protocols at the same time, such as mutual authentication, key escrow, and V2V communication issues, which caused our execution running time to be a little long. Specifically, in the pseudonym generation phase, we adopt double TA to generate users' pseudonyms, and the process of transmitting information is encrypted with public keys. Compared with existing protocols, most of the user's identity information is transmitted through a secure channel [6, 19, 21, 32, 33], and our scheme is more suitable for real environments. This phase takes about 36.5028 ms. Then, we adopt a bilinear pair to achieve mutual authentication, which is optional. The vehicle can choose whether to verify the identity of TA. It consumes about 4.21 ms. Most of the existing protocols only carry out the identity authentication between vehicles and TA [31–33]. We use three public key encryptions to realize the authentication between vehicles and the generation of the session key. After that, the communication content of the vehicle is protected by the symmetric encryption key. No one else can know the content of the message. The authentication between vehicles consumes about 16.5739 ms. The computational cost is shown in Table 4. If the proposed protocol also adopts a secure channel for registration and only performs authentication between vehicles and TA, it only takes 0.004 ms to complete the registration. The computational cost comparison is shown in Figure 4. Note that in

Table 4: Our computational cost under realistic conditions.

Phase	Execution time (ms)
Registration phase (public channel)	36.5028
Mutual authentication	4.2100
V2V authentication and communication	16.5739
Total	57.2867

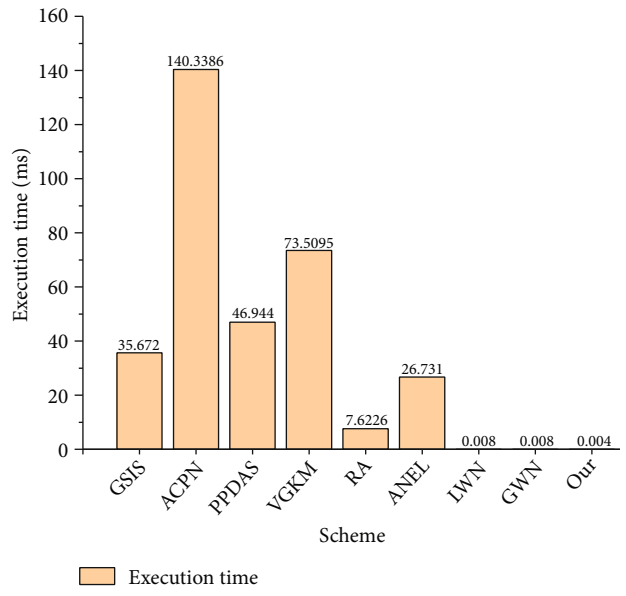

Figure 4: Authentication process in a secure channel.

the process of authentication and pseudonym generation, ACPN [7] adopts multiple signature operations, and VGKM [31] uses public key encryption and decryption operations, so their execution time is extremely long compared with other protocols.

7. Conclusion

In this paper, we propose an identity-based mutual authentication model for improving the security and privacy of communication vehicles in VANETs. IBMA is an identity-based anonymous authentication scheme which adopts identity-based encryption to reduce the storage cost of the system and solves the common key escrow problems in identity-based encryption. In addition, in order to further protect the sensitive and private information of vehicles, the central authority in this scheme is semitrusted rather than completely trusted. IBMA achieves a set of desired properties, such as mutual authentication, vehicle-to-vehicle communication, identity tracing, and resistance to various attacks. In our future work, we will explore more efficient encryption algorithms and key generation algorithms to further improve the efficiency of IBMA.

Data Availability

Data is available from http://crypto.stanford.edu/pbc/.

Conflicts of Interest

The authors have no conflict of interest to declare.

References

[1] E. R. Cavalcanti, J. A. R. de Souza, M. A. Spohn, R. C. M. Gomes, and A. F. B. F. da Costa, "VANETs' research over the past decade," *ACM SIGCOMM Computer Communication Review*, vol. 48, no. 2, pp. 31–39, 2018.

[2] S. Mathur, T. Jin, N. Kasturirangan, J. Chandrasekaran, M. G. Xue, and W. Trappe, "Parknet: drive-by sensing of road-side parking statistics," in *in Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services (MobiSys 2010)*, pp. 123–136, San Francisco, California, USA, 2010.

[3] W. Viriyasitavat, F. Bai, and O. K. Tonguz, "Toward end-to-end control in vanets," in *in 2011 IEEE Vehicular Networking Conference, IEEE VNC 2011*, pp. 78–85, Amsterdam, The Netherlands, 2011.

[4] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[5] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3765–3775, 2021.

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

[7] J. Li, H. Lu, and 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, 2015.

[8] T. Markmann, T. C. Schmidt, and M. W. Ahlisch, "Federated end-to-end authentication for the constrained internet of things using IBC and ECC," in *in Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, SIG-COMM 2015*, pp. 603-604, London, United Kingdom, 2015.

[9] Y. Tseng, J. Chen, and S. Huang, "A lightweight leakage-resilient identity-based mutual authentication and key exchange protocol for resource-limited devices," *Computer Networks*, vol. 196, p. 108246, 2021.

[10] T. Ogawara, Y. Kawahara, and T. Asami, "Disaster-tolerant authentication system for NDN using hierarchical id-based encryption," in *in 2013 21st IEEE International Conference on Net-work Protocols, ICNP 2013*, pp. 1-2, G'ottingen, Germany, 2013.

[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *in Advances in Cryptology, Proceedings of CRYPTO'84*, pp. 47–53, Santa Barbara, California, USA, 1984.

[12] T. H. Yuen, W. Susilo, and Y. Mu, "How to construct identity-based signatures without the key escrow problem," *International Journal of Information Security*, vol. 9, no. 4, pp. 297–311, 2010.

[13] Y. Huang, K. Fan, and W. Hsieh, "Message authentication scheme for vehicular ad-hoc wireless networks without RSU," *Inf. Hiding Multim. Signal Process*, vol. 6, no. 1, pp. 113–122, 2015.

[14] J. Zhou, Z. Cao, Z. Qin, X. Dong, and K. Ren, "LPPA: lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based Services in vanets," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 420–434, 2020.

[15] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in vanets," *IEEE*

Transactions on Information Forensics and Security, vol. 16, pp. 1681–1695, 2021.

[16] X. Feng, Q. Shi, Q. Xie, and L. Liu, "An efficient privacy-preserving authentication model based on blockchain for VANETs," *Journal of Systems Architecture*, vol. 117, 2021.

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

[18] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: an efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.

[19] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an iov paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, 2017.

[20] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking together efficient authentication, revocation, and privacy in vanets," in *in Proceedings of the Sixth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON 2009*, pp. 1–9, Rome, Italy, 2009.

[21] W. Jiang, F. Li, D. Lin, and E. Bertino, "No one can track you: randomized authentication in vehicular ad-hoc networks," in *in 2017 IEEE International Conference on Pervasive Computing and Communications, PerCom 2017*, pp. 197–206, Kona, Big Island, HI, USA, 2017.

[22] D. Chaum and E. van Heyst, "Group signatures," in *in Advances in Cryptology-EUROCRYPT'91, Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 257–265, Brighton, UK, 1991.

[23] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *in INFOCOM 2008. 27th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies*, pp. 1229–1237, Phoenix, AZ, USA, 2008.

[24] C. D. Jung, C. Sur, Y. Park, and K. H. Rhee, "A robust conditional privacy-preserving authentication protocol in VANET," in *in Security and Privacy in Mobile Information and Communication Systems, First International ICST Conference, Mobi Sec*, pp. 35–45, Turin, Italy, 2009.

[25] S. K. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[26] A. Malik and B. Pandey, "Security analysis of discrete event based threat driven authentication approach in VANET using petri nets," *Int. J. Netw. Secur.*, vol. 20, no. 4, pp. 601–608, 2018.

[27] J. Li, Y. Liu, Z. Zhang, B. Li, H. Liu, and J. Cheng, "Efficient id-based message authentication with enhanced privacy in wireless ad-hoc networks," in *in 2018 International Conference on Computing, Networking and Communications, ICNC 2018*, pp. 322–326, Maui, HI, USA, 2018.

[28] M. A. Alazzawi, H. A. H. Al-behadili, M. N. S. Almalki, A. L. Challoob, and M. A. Shareeda, "ID-PPA: robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network," in *in Advances in Cyber Security-Second International Conference, ACeS 2020*, pp. 80–94, Penang, Malaysia, 2020.

[29] A. Asari, M. R. Alagheband, M. Bayat, and M. R. Asaar, "A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems," *Computer Networks*, vol. 185, p. 107599, 2021.

[30] F. R. Asl and R. Samavi, "Synorm: symmetric non repudiated message authentication in vehicular ad hoc networks," in *in 86th IEEE Vehicular Technology Conference, VTC Fall 2017*, pp. 1–5, Toronto, ON, Canada, 2017.

[31] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2016.

[32] Z. Benyamina, K. Benahmed, and F. Bounaama, "ANEL: A novel efficient and lightweight authentication scheme for vehicular ad hoc networks," *Computer Networks*, vol. 164, p. 106899, 2019.

[33] H. Vasudev and D. Das, "P-SHARP: privacy preserving secure hash based authentication and revelation protocol in IoVs," *Computer Networks*, vol. 191, p. 107989, 2021.

[34] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis, S. V. Krishnamurthy, and M. Faloutsos, "Coping with packet replay attacks in wireless networks," in *in Proceedings of the 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON 2011*, pp. 368–376, Salt Lake City, UT, USA, 2011.

[35] A. Hottung and K. Tierney, "Neural large neighborhood search for the capacitated vehicle routing problem," in *in ECAI 2020-24th European Conference on Artificial Intelligence*, pp. 443–450, Santiago de Compostela, Spain, 2020.

[36] C. Hazay, G. L. Mikkelsen, T. Rabin, T. Toft, and A. A. Nicolosi, "Efficient RSA key generation and threshold paillier in the two-party setting," *Journal of Cryptology*, vol. 32, no. 2, pp. 265–323, 2019.

[37] J. Harrison, "Formalizing an analytic proof of the prime number theorem," *Journal of Automated Reasoning*, vol. 43, no. 3, pp. 243–261, 2009.

[38] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC Press, Second Edition edition, 2014.

[39] J. M. Pollard, "Monte Carlo methods for index computation (*modp*)," *Mathematics of Computation*, vol. 32, no. 143, pp. 918–924, 1978.

[40] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *in 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, Santa Fe, New Mexico, USA, 1994.

[41] T. Wu, S. Li, and L. Liu, "Fast RSA decryption through high-radix scalable Montgomery modular multipliers," *Science China Information Sciences*, vol. 58, no. 6, pp. 1–16, 2015.