electronics

MDPI

Article

Key Updatable Cross-Domain-Message Anonymous Authentication Scheme Based on Dual-Chain for VANET

Mei Sun *, Dongbing Zhang, Yuyan Guo and Xudong Zhai

School of Computer Science and Technology, Huaibei Normal University, Huaibei 235000, China
* Correspondence: sunmei109@163.com

Abstract

Traditional VANET authentication schemes often face challenges such as centralization bottlenecks and the updating of vehicle keys or pseudonyms. This paper proposes a layered approach that divides VANET into regions, utilizing dual-blockchain to enable anonymous message authentication between vehicles and RSUs, as well as between vehicles within the VANET. Compared to traditional blockchain authentication methods, this paper introduces an approach that enhances authentication efficiency and ensures information security by establishing secure connections between private and consortium chains through a trusted authority (TA). By leveraging third-party public parameter updates, the automatic updating of private and public keys for VANET nodes is achieved without the need for certificate issuance and updates. This approach facilitates long-term anonymous authentication and communication between VANET nodes, reduces the frequency of authentication interactions, simplifies authentication processes, and lowers computational and communication costs. The proposed scheme is well-suited for practical VANET environments that require low authentication latency and robust large-scale privacy protection.

Keywords: anonymous message authentication; blockchain; cross domain; VANET

1. Introduction

A VANET represents a typical intelligent transportation system, offering users convenient, safe, and intelligent travel services. Its network architecture is an open, decentralized, self-organizing mobile ad hoc network that supports multi-hop forwarding, accommodates rapid node movement, and meets strict latency requirements. Due to their unique network structures and wireless communication methods, VANETs are susceptible to various network attacks in practical applications. To safeguard the security and privacy of VANET communication entities, it is imperative to authenticate entities and messages while protecting vehicle locations and trajectory information. Therefore, communication and message authentication must incorporate privacy protection functions. In recent years, scholars have proposed several authentication protocols for VANET, which can be categorized into a few main types. In public key infrastructure (PKI)-based schemes, multiple certificates are required to achieve authentication anonymity by obscuring the vehicle's true identity. However, the extensive use of anonymous certificates complicates certificate management and revocation, necessitating the participation of a management center in authentication, which can easily create a system bottleneck [1–3]. Identity-based password authentication schemes in VANET such as those outlined in [4–9], often require the system key to be stored in the vehicle's tamper-proof device (TPD) to maintain authentication anonymity. In these schemes, the system key and vehicle pseudonym are used to generate the authentication

Academic Editors: Paris Kitsos and Hung-Yu Chien

Received: 24 February 2026
Revised: 23 March 2026
Accepted: 3 April 2026
Published: 7 April 2026

key, with the pseudonym verifying identity to achieve anonymity. However, TPDs require high security [4,5,7]. Other schemes, including those in [8,10–16], do not require TPDs; however, to maintain anonymity during communication, vehicles frequently communicate with authoritative institutions or TAs to update pseudonyms or vehicle private keys. Blockchain technology offers a solution by enabling distributed data storage, peer-to-peer transmission, consensus mechanisms, and encryption algorithms, making it suitable for decentralized application environments with distributed consensus, especially in complex road traffic settings where vehicles do not inherently trust each other. Currently, there are numerous blockchain based authentication solutions for VANET, many of which address anonymous authentication between vehicles and RSUs or infrastructure [17–19], but they are unable to provide anonymous authentication between vehicles. Additionally, there are various schemes, where the vehicle and RSU or infrastructure authentication require application of the private key to a third-party authority, leading to excessive communication interactions, authentication delays and other issues. This paper proposes a dual-chain and cross-region anonymous authentication and communication scheme, that stratifies VANET and divides multiple regions. It achieves cross-region anonymous authentication and communication between vehicles and RSUs or infrastructures, as well as between vehicles themselves through the joint work of dual blockchains such as private chain and alliance chain. The vehicle can automatically update its authentication private key and public key based on the public parameters released by the third-party authority, which shortens the authentication delay and reduces the interaction times and complexity of authentication.

2. Related Work

Currently, numerous solutions utilize blockchain technology to address the decentralization challenges in VANET authentication. In 2019, Yao et al. [20] proposed a cross-domain anonymous authentication scheme for the Internet of Vehicles based on blockchain technology; however, the pseudonyms used in vehicle communications are static, rendering the scheme non-linkable. Wazid [21] employed fog computing to design a lightweight authentication key agreement protocol suitable for the Internet of Vehicles environment; however, this solution does not adequately address the security issues of lightweight authentication password protocols, such as desynchronization attacks. Shen et al. [22] introduced a blockchain-assisted IoT declaration security authentication mechanism that effectively reduces the overhead associated with cross-message authentication. Yang et al. [23] proposed a blockchain-based multidomain authentication scheme for the Internet of Vehicles that reduces the computational overhead associated with pseudonyms and key generation. Liu et al. [24] developed a dual-layer sharded-blockchain cross-authentication scheme, while Sabjeev et al. [25] proposed a blockchain-assisted authentication and secure communication scheme; both primarily address authentication between vehicles and RSUs. This study proposes a blockchain-assisted vehicle networking authentication mechanism with a hierarchical dual-chain public key system that can be updated automatically. It enables anonymous message authentication and communication between vehicles and infrastructure, as well as between vehicles, and supports long-term anonymity in communication and authentication.

3. Background of Research

3.1. Preparatory Knowledge

Let F_q denote a finite field of order p, where p is a large prime number. An elliptic curve is defined as $E : y^2 = x^3 + ax + b \bmod p$ where $a, b \in F_p$. G denotes the set of points of order q defined on the elliptic curve E, with the generator P. G includes an infinite point O, and it possesses the following properties:

Addition (+): Let P and Q be two points on G. If $P \neq Q$, then $R = P + Q$, and R is the intersection point of E and the line connecting P and Q. If $P = Q$, then $R = P + Q$, and R is the intersection point of E and the tangent to $P(Q)$. If $P = -Q$, then $R = P + Q = O$.

Scalar multiplication (.): Let $P \in G$ and $m \in Z_q^*$. Then the scalar multiplication on G is defined as $mP = P + P + \ldots + P$ (m times).

Definition 1. *The elliptic curve discrete logarithmic problem (ECDLP). Let G be a finite cyclic group on the elliptic curve E with order being a large prime number q, where P is the generator of G and Q is a point of G. The goal of ECDLP is to calculate the solution x satisfying $Q = xP$, where $x \in Z_q^*$.*

Definition 2. *In the elliptic curve computational Diffie–Hellman problem (ECDHP), let G be a finite cyclic group on the elliptic curve E with order being a large prime number q, where P is the generator of G, and for any $aP, bP \in G$, the Elliptic Curve Computational Diffie-Hellman problem (ECDHP) is defined as the task of computing the point $abP \in G$ within polynomial time t, where $a, b \in Z_q^*$.*

If an algorithm cannot solve the ECDLP problem or the ECDHP problem on group G within time t with a non-negligible probability ε, then the ECDLP problem or the ECCDH problem is said to be difficult in group G.

3.2. System Model

To address the issues of anonymous authentication and communication between vehicles and between vehicles as well as infrastructure, this study employs a layered, partitioned, and dual-chain blockchain structure. As illustrated in Figure 1, the core layer primarily consists of highly secure trusted authorities (TAs) and high-performance servers that handle the registration of vehicles and RSUs, maintain the real identity information of vehicles and RSUs, store temporary public keys, and generate and store secret parameters for negotiations between vehicles and RSUs. This layer utilizes a private blockchain as an information platform to implement distributed storage and synchronization of information among various TAs. The core layer maintains one primary chain, referred to as the registration information chain, which manages the registration data, identity information, and keys negotiated between vehicles and TAs, as well as between RSUs and TAs. The management layer maintains one consortium chain, known as the global temporary public key chain, which maintains temporary public keys of vehicles and RSUs, provides cross-domain authentication services, and stores the public keys of vehicles and RSUs along with their validity periods, region IDs, and the corresponding vehicle addresses in the registration information chain. The management layer comprises TAs, RSUs, vehicles, and edge nodes, which are divided into regions based on their locations. Each region utilizes a consortium blockchain as its information platform, which stores temporary public keys for vehicles and RSUs, and assigns a regional area identification (AID). The TA is part of both the core and management layers and is responsible for maintaining information on both private and consortium chains. Within the consortium chain, the TA functions as the full node of the blockchain, storing temporary public keys and other relevant information from multiple regional vehicles and RSUs. RSUs and edge nodes, serving as partial nodes, primarily store temporary public keys and validity periods for vehicles and RSUs in their respective regions. To enhance the maintenance efficiency of the consortium chain, data management is handled by the TA and RSUs, while vehicles are restricted to data access without participating in the consensus mechanism. RSUs and edge nodes also take part in consensus within the consortium chain, whereas other network nodes are limited to querying data. Due to the relatively small number of RSUs and edge nodes in each region,

data are maintained by a limited set of nodes, resulting in high operational efficiency of the consortium chain. Although network nodes can query public keys, they are unable to determine the true identity of a vehicle from its public key, thus preserving the anonymity of authentication.

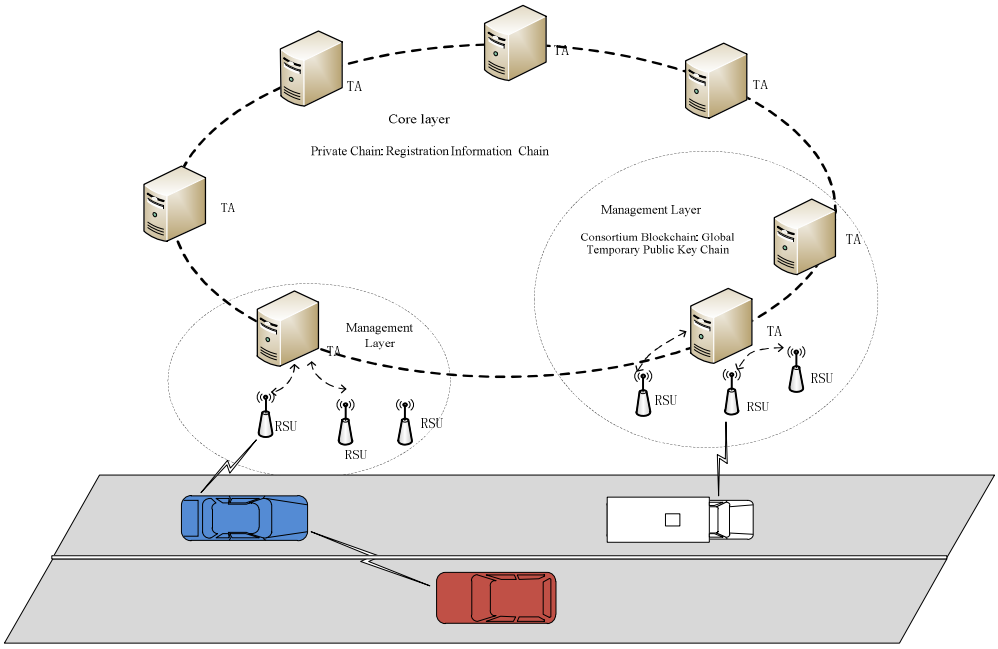

Figure 1. VANET network structure.

The global temporary public key chain utilizes the Proof of Authority (POA) pre-authorization algorithm inherent to consortium blockchains. All TA nodes generate blocks for the global temporary public key chain in strict compliance with the pre-authorized sequence. RSUs and certain edge nodes endowed with strong robust computational capabilities employ smart contract algorithms to download blocks containing temporary public key information pertaining to nodes within their designated regions. Vehicles and other nodes accomplish authentication by querying the temporary public key blocks specific to their regions or by accessing the temporary public key information embedded within the blocks of the global temporary public key chain.

During the registration phase, the Trusted Authority (TA) employs a smart contract to compute a series of secret parameters for both the vehicle and the Roadside Unit (RSU), drawing upon the parameters furnished by them. The vehicle and the RSU each securely retain their respective secret parameters, while the TA proceeds to upload the registration information along with these secret parameters onto the registration information chain. Utilizing the secret parameters computed during the registration process, the TA then calculates multiple temporary public keys for both the vehicle and the RSU, subsequently uploading these keys onto the global temporary public key chain. To guarantee the anonymity and unlinkability of vehicles, each vehicle is allocated multiple temporary public keys. When a vehicle engages in authenticated communication with other nodes (encompassing vehicles and RSUs), it signs messages using its secret parameters. Other nodes ascertain the authenticity and reliability of these messages by verifying the existence of a corresponding temporary public key for the vehicle within the global temporary public key chain. To uphold long-term anonymity in vehicle authentication, the TA periodically disseminates secret update parameters via the smart contract and records these key update parameters onto the registration information chain. Vehicles then update their secret parameters and temporary public keys based on these secret update parameters. The TA

updates the temporary public keys of vehicles in the global temporary public key chain by utilizing the original secret parameters and secret update parameters sourced from the registration information chain. The updating of vehicle temporary public keys does not necessitate information exchange with the TA. Long-term anonymity and unlinkability in vehicle authentication and communication can be attained through the utilization of multiple temporary public keys and their regular updates.

4. Cross-Domain Message Authentication Scheme Based on VANET

The symbol definitions for this article are as Table 1:

Table 1. The Symbol Definitions.

Symbol	Definition
$\{G, P, q\}$	Cyclic addition group G, generator of cyclic addition group P, the order of addition group q
s	System Private Key
P_{pub}	System Public Key
H_0, H_1, H_2, H_3, H_4	Secure hash function
P_r	Key update parameters
x_t	Shared key between vehicle and TA
P_{vt}	Temporary public key for vehicles
x_{uj}	Shared key between RSU and TA
P_{uj}	RSU temporary public key
PID_m	Vehicle pseudonym
AID_i	Area ID
RID_i	Vehicle ID
RSU_{id}	RSU ID
r, u_j, v_t, w_m, w_l	Random number
$T_{\exp r}, T_{\exp}$	Time stamp

4.1. System Initialization

Given the safety parameter k, the TA chooses a cyclic addition group $\{G, P, q\}$ and generates the system key s. The public key $P_{pub} = sP$ is then calculated. The secure hash functions used include $H_0 : \{0,1\}^* \to Z_q^*$, $H_1 : G \to Z_q^*$, $H_2 : \{0,1\}^* \times G \times G \times \{0,1\}^* \to Z_q^*$, $H_3 : G \times \{0,1\}^* \to Z_q^*$, and $H_4 : G \times G \times \{0,1\}^* \to Z_q^*$. The TA publishes the system parameter $\left\{G, P, P_{pub}, q, H_0, H_1, H_2, H_3, H_4\right\}$ to the registration information chain of the core layer (CL) and broadcasts these parameters within the VANET system. To maintain security and facilitate regular updates, the TA regularly selects a random number r for the region and calculates the updated public key $P_r = rP$ using $(r, P_r, AID_i, T_{\exp r})$ as the key update parameter, where $T_{\exp r}$ represents the start and end times of P_r usage on the network. AID_i represents the region of P_r. The TA uploads the key update parameter $(r, P_r, AID_i, T_{\exp r})$ to the registration information chain and broadcasts $(P_r, AID_i, T_{\exp r})$ to the VANET system.

4.2. Vehicle Registration

The vehicle provides owner information, its real ID, license plate number, and the AID to which it belongs, and submits a registration application to the TA through a secure channel. The vehicle selects k random numbers $v_t (t = 1, 2 \cdots k)$ for the vehicle and calculates $P_t = v_t P$; it then sends P_t to the TA through a secure channel. The TA selects the currently valid parameter $(r, P_r, AID_i, T_{\exp r})$ for the current region and calculates multiple original shared keys $x_t = H_1(rP_t)$ between the TA and the vehicle using the provided values. The TA then calculates the temporary public key of the vehicle $P_{vt} = x_t P$. The vehicle registration process is shown in Figure 2.

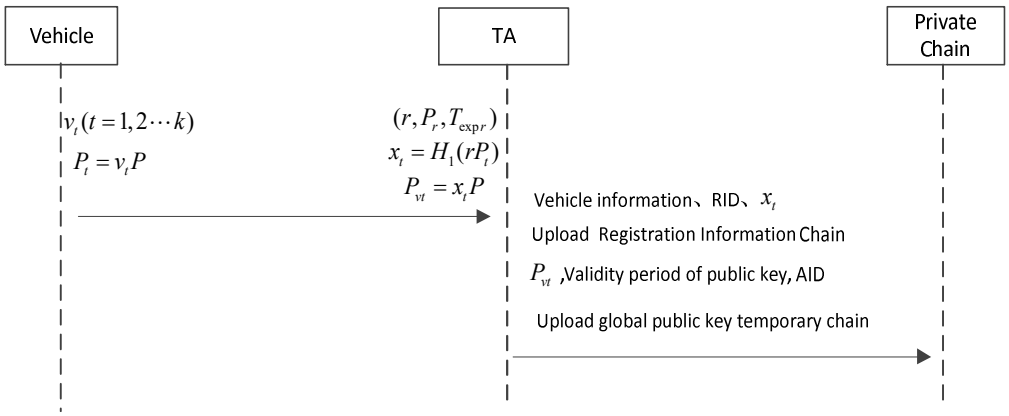

Figure 2. The Process of Vehicle Registration.

The TA uploads the owner information, real ID, and original shared key x_t of the vehicle to a private registration information chain within the core layer. Additionally, the TA uploads the temporary public key $(P_{vt}, T_{\exp r})$ of the vehicle to the global temporary public key chain in the management layer, which mainly provides cross-domain validation services for vehicles. Finally, the TA sends an acknowledgment $(P_r, AID_i, T_{\exp r})$ to the vehicle. Upon receiving the acknowledgment, the vehicle calculates the shared keys $x_t = H_1(v_t P_r)$ and its temporary public key $P_{vt} = x_t P$ based on the information from the TA, and securely stores them for future authentication and communication purposes.

4.3. RSU Registration

The RSU_j chooses a random number u_j, calculates $P_{uj} = u_j P$, and sends its location information, identity information ID, area ID AID_i, and P_{uj} to the TA through a secure channel. After validating the submitted information, the TA selects the currently valid system parameter $(r, P_r, AID_i, T_{\exp r})$ for the current region and calculates the original shared key $x_{uj} = H_1(rP_{uj})$ between the TA and RSU. The TA then calculates the temporary public key $P_{rsuj} = x_{uj} P$ for the RSU. The TA uploads the information of the RSU and the original shared key x_{uj} to the registration information chain of the core layer. It also uploads the temporary public key P_{rsuj} of the RSU to the global temporary public key chain in the management layer. Finally, the TA sends $(P_r, AID_i, T_{\exp r})$ to the RSU. Upon receiving it, the RSU calculates the original key $x_{uj} = H_1(u_j P_r)$ and its temporary public key $P_{rsuj} = x_{uj} P$ and securely stores them for future use in authentication and communication. The RSU registration process is shown in Figure 3.

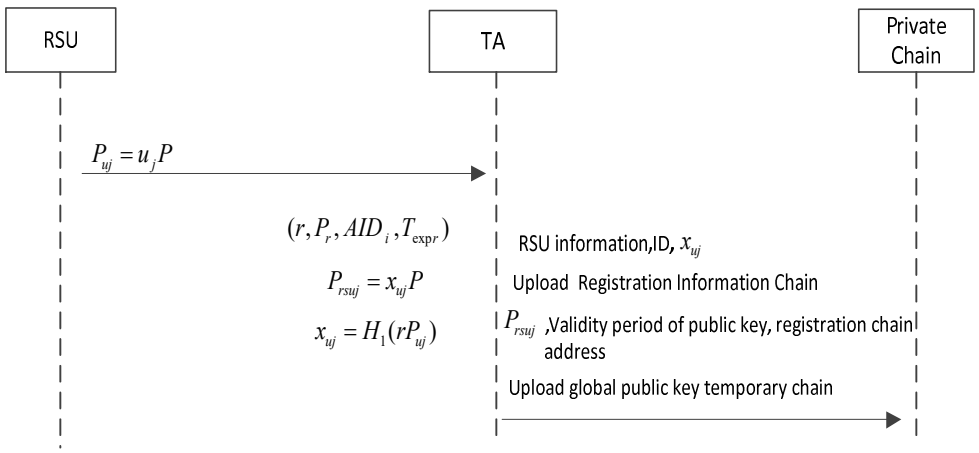

Figure 3. The Process of RSU Registration.

4.4. Cross-Domain Anonymous Message Authentication Between Vehicles and RSUs

When the vehicle V_m arrives at an area, it needs to send a message M. The vehicle selects a random number w_m and calculates its pseudonym $PID_m = RID_m \oplus H_1(w_m P_{pub})$. Next, the vehicle calculates the message signature $\delta = x_t H_2(PID_m, P_w, P_{vt}, M, AID_i, T_{\exp}) + w_m$, where x_t $(t = 1, 2, \ldots, k)$ is one of the temporary keys selected by the vehicle and negotiated with TAs, $P_w = w_m P$ and P_{vt} is the temporary public key corresponding to the temporary shared key x_t of the vehicle. AID_i is the area ID for vehicle registration and $T_{\exp}$ is the timestamp. The vehicle then sends the message $(\delta, PID_m, P_w, P_{vt}, M, AID_i, T_{\exp})$ to nearby RSUs.

Upon receiving the message, the RSU checks if the timestamp is within its validity period and verifies if Equation (1) holds.

$$\delta P = H_2(PID_m, P_w, P_{vt}, M, AID_i, T_{\exp}) P_{vt} + P_w \quad (1)$$

If Equation (1) does not hold, the message is discarded. However, if Equation (1) holds and the AID_m and RSU's region ID are not the same, the RSU sends query request $(H_3(P_{vt}, RSU_{id}, xu, T_{\exp}), RSU_{id}, P_{vt}, T_{\exp})$ to the TA in this region. Here, xu is the shared key between TAs and RSU, and RSU_{id} is the identity of the RSU. The TA then queries P_{vt} the global temporary public key chain in the management layer for the temporary public key. If it is found, the TA returns the query results to the RSU through the secure channel $H_3(P_{vt}, true, xu, T_{\exp}), true$. Upon receiving a confirmation message from the TA, the RSU confirms that the message signature is valid. If P_{vt} is not found in the global temporary public key chain, the TA will return an error message $(H_3(P_{vt}, false, xu, T_{\exp}), false)$ to the RSU, indicating that the signature is invalid. The vehicle and RSU authentication process is shown in Figure 4.

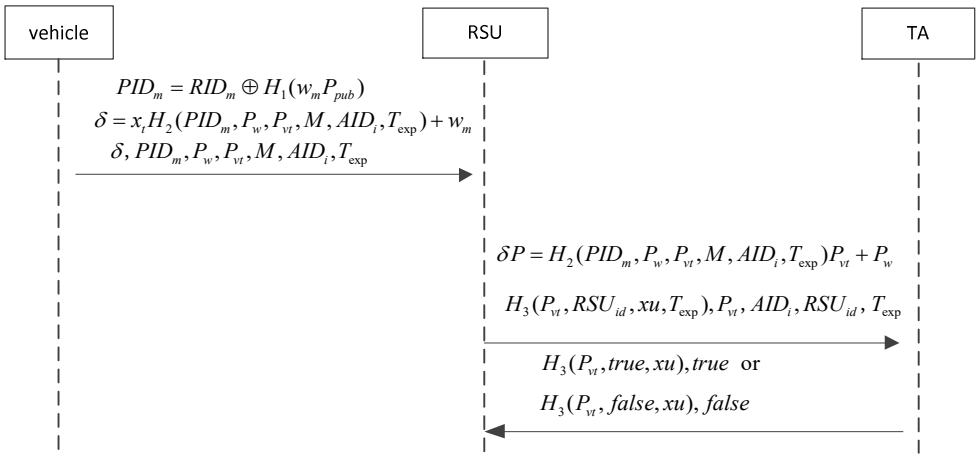

Figure 4. Cross-domain authentication process between vehicle and RSU.

4.5. Cross-Domain Anonymous Message Authentication Between Vehicles

When the vehicle V_m arrives in an area, it needs to send a message M_m. The vehicle randomly selects a random number w_m and calculates its pseudonym $PID_m = RID_m \oplus H_1(w_m P_{pub})$. V_m then calculates the message signature $\delta_m = x_t H_2(PID_m, P_w, P_{vt}, M_m, AID_i, T_{\exp}) + w_m$, where x_t is one of the temporary shared keys selected by the vehicle and negotiated with TA, $P_w = w_m P$ and P_{vt} is the temporary public key corresponding to the vehicle's temporary shared key x_t, AID_i is the area ID for vehicle registration, and $T_{\exp}$ is the timestamp. The vehicle V_m sends $(\delta_m, PID_m, P_w, P_{vt}, M_m, AID_i, T_{\exp})$ to the other vehicles.

Upon receiving the message, the other vehicle V_l checks if the timestamp is within the validity period. If the timestamp has not expired, it verifies if Equation (2) holds.

$$\delta_m P = H_2(PID_m, P_w, P_{vt}, M_m, AID_i, T_{\exp}) P_{vt} + P_w \quad (2)$$

If Equation (2) holds, the receiving vehicle determines whether the sending vehicle and itself are in the same area. If they are, it queries the local consortium blockchain, if P_{vt} is found, then the signature is valid. If the vehicle V_l and the other vehicle V_m are not in the same area, the vehicle V_l chooses a random number w_l and calculates $PID_l = RID_l \oplus H_1(w_l P_{pub})$ and $P_l = w_l P$. The vehicle V_l then sends a query request $(H_4(P_{vt}, P_l, PID_l, x), PID_l, P_{vt}, P_l, T_{\exp})$ to the TA in the current area. The TA calculates $RID_l = PID_l \oplus H_1(sP_l)$ and obtains the original shared key x between the vehicle and TA based on RID_l. The TA then verifies whether $H_4(P_{vt}, P_l, PID_l, T_{\exp}, x)$ is valid. If it is established, the TA queries whether P_{vt} exists in the global temporary public key chain, if it is found, the TA returns a confirmation message $H_3(P_{vt}, true, PID_l, x, T_{\exp}), true$ to the vehicle V_l, and adds P_{vt} to the local consortium chain. After the vehicle V_l receives the confirmation, it recognizes that the signature of the confirmation message is valid. If P_{vt} is not found in the global temporary public key chain, the TA returns an error message $H_3(P_{vt}, false, PID_l, x, T_{\exp}), false$ to the vehicle V_l, indicating that the signature is invalid. The vehicle and vehicle authentication process is shown in Figure 5.

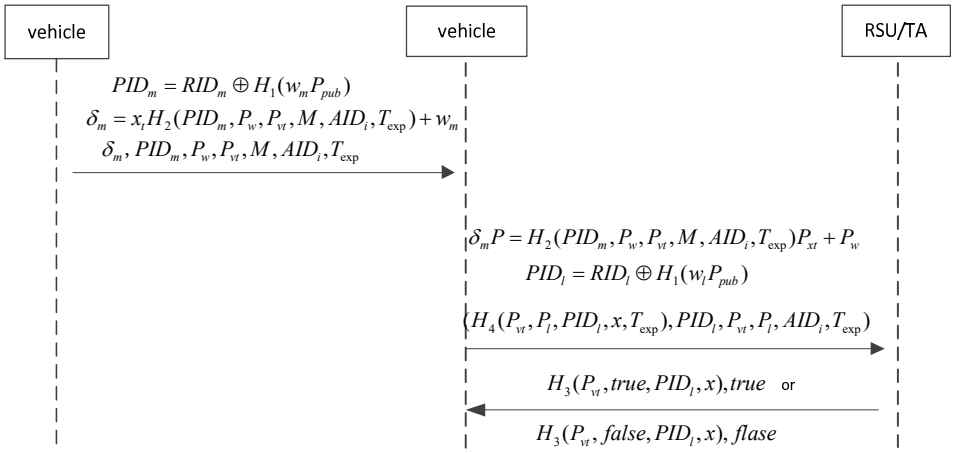

Figure 5. Vehicle and vehicle cross-domain authentication process.

4.6. Batch Authentication of Message

When the RSU receives n message signatures $\{\delta_m, PID_m, P_{wm}, P_{vmt}, M_m, AID_i, T_{\exp m}\}_{m=1}^{n}$ from different vehicles simultaneously, the RSU calculates $\mu_m = H_2(PID_m, P_{wm}, P_{vmt}, M_m, AID_i, T_{\exp m})$ and verifies if Equation (3) holds.

$$\sum_{m=1}^{n} \delta_m P = \sum_{m=1}^{n} \mu_m P_{vmt} + \sum_{m=1}^{n} P_{wm} \quad (3)$$

If Equation (3) holds, the public key $P_{wm}(m = 1, 2, \cdots n)$ is queried to determine whether it exists in the blockchain. If it is found in the blockchain, the message signature is considered valid. However, if the public key is not found, the batch authentication fails.

4.7. Update of Temporary Public Key for Vehicles

TA selects a new random number r' for the region and calculates $P'_r = r'P$, $\sigma = sH_3(P'_r, AID_i, T_{\exp r}) + r'$. In VANET system, the TA broadcasts $(\sigma, P'_r, AID_i, T_{\exp r})$ to the region, where $T_{\exp r}$ is the duration of use for P'_r, AID_i is the area identifier for the current region. Upon receiving this broadcast, the vehicle verifies whether Equation (4) holds.

$$\sigma P = H_3\left(P'_r, AID_i, T_{expr}\right) P_{pub} + P'_r \quad (4)$$

If Equation (4) is established, the vehicle uses the original shared keys x_t $(t = 1, 2, \ldots, k)$ to calculate new temporary shared keys $x'_t = H_3(x_t P'_r, x_1, x_2 \ldots x_k)$ and new temporary

public keys $P'_{vt} = x'_t P$; here $t = 1, 2, \ldots, k$, $x_1, x_2 \ldots x_k$ represents the sequence generated using the original shared keys.

Simultaneously, the TA calculates the new temporary shared keys $x'_t = H_3(x_t P'_r, x_1, x_2, \cdots x_k)$ based on the original shared keys x_t of the vehicle stored in the registration information chain of the private chain; here $t = 1, 2, \ldots, k$. The TA then calculates the corresponding new temporary public keys $P'_{vt} = x'_t P$ ($t = 1, 2, \ldots, k$). The TA uploads the new temporary public keys $(P'_{vt}, T_{\exp r})$ ($t = 1, 2, \ldots, k$) to the corresponding region of the global temporary public key chain.

5. Security Analysis

Anonymity: In the proposed scheme, the vehicle sends message signatures using its pseudonym $PID_i = RID_i \oplus H_1(w_i P_{pub})$, where the real identity is hidden within a pseudonym. For other vehicles or RSUs, the real identity remains hidden. Given $P_{pub} = sP$ and $P_{wi} = w_i P$, the discrete logarithm problem on elliptic curves (ECDLP) makes it computationally infeasible to determine w_i and s. Without knowing the random numbers w_i and s, it is impossible to calculate $w_i P_{pub} = w_i sP$ according to ECDHP or recover the true name RID_i of the vehicle. Only the TA has the capability to restore the true identity of the vehicle $RID_i = PID_i \oplus H_1(sP_{wi})$ from a pseudonym.

Unlinkability: In the proposed scheme, the vehicle employs pseudonyms and temporary public keys for message signing. Each pseudonym used by the vehicle is unique for every signature, and the vehicle has multiple temporary public keys at its disposal. For each message, one signature is randomly selected, and the vehicle's temporary public key is regularly updated. This approach makes it challenging for attackers or other vehicles to link the vehicle's identity across different messages, as it is difficult to correlate pseudonyms and temporary public keys from two separate message signatures.

Lemma 1. *The signed message in the Cross-domain authentication process between vehicle and RSU is unforgeable. Assuming that the ECDLP is a difficult problem, the message signature proposed in the Cross-domain authentication process between vehicle and RSU can resist adaptive chosen-message forgery attacks.*

Proof. Assume there exists an attacker A who is capable of forging a signature message of a vehicle within polynomial time with a non-negligible probability ε. Given an instance of the Elliptic Curve Diffie-Hellman (ECDLP) problem $(P, Q = xP)$, where $P, Q \in G$ and $x \in Z_q^*$, assume that there exists a challenger C acting as a solver of the ECDLP problem, who can solve it in polynomial time. □

The security model is defined as a game between Attackers A and Challenger C. Challenger C initializes the system and generates the system key s using the public key $Q = sP$. The challenger C sets system parameters paras = $\{G, P, Q, q, H_0, H_1, H_2, H_3, H_4\}$. C randomly selects a vehicle m (with an identity tag RID_m) as the identity of the challenge. The vehicle's public key is P_{vt}. Then, A adaptively proceeds to query the oracle to C. After querying the oracle, C responds to A's query in the following:

(1) $H(M_l)$ oracle query: When A initiates a query with M_l, C checks the maintained list $L_l = (M_l, h_l)$. If there is no information about M_l in the list, C selects a random number $h_l \in Z_q^*$ and adds (M_l, h_l) to the list L_l, and return h_l to A, otherwise return h_l from the list to A. Here, $l = 0, 1, 2, 3, 4$.

(2) Query vehicle pseudonym: C maintains the list $L_{pid} = (RID_k, h_1, PID_k)$. When A initiates a query with RID_k, C checks the maintained list L_{pid}, If there is no information about RID_k, C selects random number $h_1 \in Z_q^*$, and makes $PID_k = RID_k \oplus h_1$. Next C adds $L_{pid} = (RID_k, h_1, PID_k)$ to the list L_{pid}, and returns PID_k to A.

(3) Query vehicle message signature.

When A queries with $PID_k, M_k, AID_i, T_{\exp}$, if $PID_k = PID_m$, then C terminates the game. Otherwise, C selects random number $h_2, \delta \in Z_q^*$, and makes $P_w = \delta P - h_2 P_{vt}$, and then C returns (δ, h_2, P_w) to A. A receives it.

According to the bifurcation lemma [26], A selects different h_2' and generates another valid signature (δ', h_2', P_w) in polynomial time t. At this stage, the two signatures meet as follows:

$$\delta P = h_2 P_{vt} + P_w \tag{5}$$

$$\delta' P = h_2' P_{vt} + P_w \tag{6}$$

From Equations (5) and (6), we have the following:

$$(\delta - \delta')P = x_t(h_2 - h_2')P \tag{7}$$

According Equation (7), C can calculate $x_t = (\delta - \delta')(h_2 - h_2')^{-1}$, with x_t as a solution to the equation $P_{vt} = x_t P$. In the process of solving for x_t, the probability of its solution can be divided into two events:

$E1$: C terminates the game during the query on the signature message.

$E2$: C outputs a valid signature message.

Let n_s denote the number of queries made to the signature message in the game. According to the game rules, we have $\Pr(E_1) \geq (1 - 1/(n_s - 1))^{n_s}$, $\Pr(E_2|E_1) \geq \varepsilon$. The probability of solving the ECDLP problem under the random oracle model is as follows:

$$\Pr(E_1 \wedge E_2) = \Pr(E_1)\Pr(E_2|E_1) = (1 - 1/(n_s - 1))^{n_s}\varepsilon \tag{8}$$

Obviously, Equation (8) represents a non-negligible probability, which conflicts with the difficulty of the ECDLP problem. Therefore, it can be proven that the message signature proposed in the Cross-domain authentication process between vehicle and RSU can resist adaptive chosen-message forgery attacks.

Lemma 2. *The signed message in the Cross-domain authentication process between vehicles unforgeable. Assuming that the ECDLP is a difficult problem, the message signature proposed in the Cross-domain authentication process between vehicles can resist adaptive chosen-message forgery attacks.*

By a similar argument as in Lemma 1, we obtain that the signed message in the Cross-domain authentication process between vehicles is unforgeable.

Anti-forgery attack during the cross-domain query phase: If an attacker forges the vehicle private key and public key $(x_t, P_{vt} = x_t P)$, successfully forges the signature $(\delta_m, PID_m, P_w, P_{xt}, M_m, AID_i, T_{\exp})$, and makes Equation (1) hold, the RSU queries the local consortium chain or global temporary public key chain to check if P_{vt} exists. When querying P_{vt} during cross-domain queries, the RSU sends $H_3(P_{xt}, RSU_{id}, xu, T_{\exp})$ to the TA, and the TA replies with $H_3(P_{xt}, true, xu, T_{\exp}), true$ or $H_3(P_{xt}, false, xu, T_{\exp}), false$. During cross-domain queries, it is difficult for the attacker to control the consortium chain and global temporary public key chain to forge P_{vt}. Similarly, both the messages sent by the RSU and the replies from the TA require the use of the shared key xu between the RSU and TA. Without knowing xu, based on the strong collision property of the hash function, the attacker cannot construct a hash value that meets the requirements. Therefore, the vehicle and RSU cross-domain authentication scheme can resist forgery attacks.

Similarly, during cross-domain authentication between vehicles, if an attacker forges the vehicle's private key and public key $(x_t, P_{vt} = x_t P)$ and successfully forges the sig-

nature $(\delta_m, PID_m, P_w, P_{vt}, M_m, AID_i, T_{\exp})$, making Equation (2) hold, other vehicles need to query the local consortium blockchain or global temporary public key blockchain to verify whether the public key P_{vt} exists. During cross-domain authentication, the vehicle sends a public key query message $(H_4(P_{vt}, P_l, PID_l, x), PID_l, P_{vt}, P_l, T_{\exp})$ to the TA, and the TA replies with $H_3(P_{vt}, true, PID_l, x, T_{\exp}), true$ or $H_3(P_{vt}, false, PID_l, x, T_{\exp}), false$ to the vehicle. It is difficult for the attacker to control the consortium blockchain and global temporary public key blockchain to forge P_{vt}. Without knowing the shared key x between the vehicle and the TA, the attacker cannot forge the message sent by the vehicle and the message replied by the TA based on the collision resistance of the hash function. Therefore, the blockchain-based cross-domain query scheme proposed in this paper can resist forgery attacks.

Theorem 1. *Lemmas 1 and 2 reveal that when the ECDLP problem is difficult, the opponent cannot forge the authentication message. Based on the security analysis of cross-domain queries, if the hash function has strong collision resistance, the proposed solution can resist forgery attacks. Thus, the authentication scheme proposed can resist the adaptive selection message forgery attack.*

Traceability: During vehicle authentication, if it is discovered that vehicle V_m is sending a malicious message, the signature $(\delta, PID_m, P_w, P_{vt}, M, AID_i, T_{\exp})$ of the message is sent to the TA. The TA can recover the real ID of the vehicle using pseudonym and system private keys. According to $PID_i = RID_i \oplus H_1(w_i P_{pub})$, the TA can recover the real ID $RID_i = PID_i \oplus H_1(sP_{wi})$ through the system key s. The TA can then locate the address corresponding to the temporary public key P_{vt} of the vehicle in the global registration information chain through the global temporary public key chain. The TA can find the original real ID of the vehicle by finding the address and identifying the real vehicle. Even if $PID_i = RID_i \oplus H_1(w_i P_{pub})$ and $(\delta, PID_m, P_w, P_{vt}, M, AID_i, T_{\exp})$ have expired, the TA can still calculate the vehicle's public key at the time of the incident using the original shared key and the updated key parameters stored in the information registration chain. This allows the TA to retrieve the vehicle's real ID and related information. The reference [27] offers a time-aware LSTM model for detecting criminal activities in blockchain transactions on monitoring changes. It provides a basis for detecting harmful behaviors through transaction patterns. The blockchain transaction behavior discussed can be subjected to crime detection using this method before starting the identity recovery process. Therefore, the proposed scheme satisfies the traceability requirements.

Resist common attacks: The proposed scheme employs a private key to digitally sign messages, providing resistance against message-tampering attacks. Because only the vehicle possessing its private key can generate a valid message signature, the scheme effectively resists impersonation attacks. Additionally, the messages, key update parameters, and query requests used in this study are all timestamped, ensuring the freshness of the messages and providing protection against replay attacks. Communications between the vehicle and TA, as well as between the RSU and TA, utilize original shared keys, which further bolster security by effectively resisting attacks such as forgery, impersonation, and man-in-the-middle attacks. A security comparison of various schemes is presented in Table 2.

Forward security analysis of cryptographic keys: To prevent the leakage of r from compromising the security of the entire network for a certain period of time, we modify the scheme so that each region maintains a separate r. This way, even if r is leaked, it will only affect the security of one region for a certain period of time. To enhance the security of vehicle keys, the scheme proposed in this paper utilizes k original shared keys $x'_t = H_3(x_t P'_r, x_1, x_2, \ldots x_k), i = 1, 2, \ldots, k$. It employs these k shared keys and the region update parameter P_r to collectively update the vehicle's individual key. The compromise of

the vehicle's individual key only affects the signature at a specific moment. Attackers are unable to update the key based on the updated parameters, thus preventing them from forging future signatures.

Table 2. Comparison of Scheme Security.

Scheme	Anonymity	Unlinkability	Unforgeability	Traceability	Resist Common Attacks	Batch Cross-Domain Authentication
Bayat et al.'s [7]	Yes	Yes	Yes	Yes	Yes	Yes
Yang et al.'s [23]	Yes	Yes	Yes	Yes	Yes	No
Liu et al.'s [24]	Yes	Yes	Yes	Yes	Yes	Yes
Shen et al.'s [22]	No	No	Yes	Yes	Yes	No
This article's proposal		Yes	Yes	Yes	Yes	Yes

6. Performance Analysis and Evaluation

6.1. Calculate Overhead

Section 6.1 evaluates the performance of the proposed scheme in terms of message signatures, message signature verification, and batch verification, comparing and analyzing it against other studies. All operations in the scheme are based on elliptic curve calculations, utilizing cryptographic algorithms implemented with the MIRACL library. In order to compare at the same security level, we construct two 80-bit security level cryptographic operation schemes. Bilinear pair cryptographic schemes are set as follows: $e : G_1 \times G_1 \to G_2$, $\overline{E} : y^2 = x^3 + ax + b \bmod \overline{p}$ is a hyper singular curve with degree 2, where $\overline{p}$ is a 512-bit prime. G_1 is an additive group based on $\overline{E}$ with order $\overline{q}$; $\overline{P}$ is the generator of G_1 with order $\overline{q}$. The same security level of elliptic curve cryptography is set as follows: $E : y^2 = x^3 + ax + b \bmod p$ is a non-super singular elliptic curve, where p and q are 160-bit primes, $a, b \in Z_q^*$. G is an additive group on E. P is the generator of G with order q. The evaluations were conducted on a Windows 10 platform equipped with 8GB of memory and a CPU running at a clock speed of 2.5 GHz. The primary calculation operation is executed 1000 times to derive the average value. The primary operations and their corresponding computational times are detailed in Table 3. The computational costs of different schemes are shown in Table 4.

Table 3. Execution Time of Encryption Operations.

Cryptographic Operation	Computing Time (ms)
Bilinear pairing operation T_{bp}	6.3743
Bilinear dot multiplication operation T_{sm}	0.7741
Bilinear point addition operation T_{pa}	0.0346
Modular exponentiation T_{ep}	3.2236
Elliptic curve multiplication operation T_{mul}	0.7757
Elliptic curve addition operation T_{add}	0.0073
Unidirectional hash function operation T_h	0.0004

The pseudonyms $PID_m = RID_m \oplus H_1(w_m P_{pub})$ used in this article are calculated offline by the vehicles, with no partial key calculation involved. The vehicle keys are derived using public key parameters published by TA. Specifically, the TA calculates $P'_r = r'P$ and $\sigma = sH_3(P'_r, AID_i, T_{\exp}) + r'$ whether the vehicle's verification equation holds, $\sigma P = H_3(P'_r, AID_i, T_{\exp})P_{pub} + P'_r$. If the verification equation is established, the vehicle uses the original shared key x_t to calculate a new temporary shared key $x'_t = H_3(x_t P'_r, x_1, x_2 \ldots x_k)$ and a new temporary public key $P'_{vt} = x'_t P$. The public key for the vehicle is then updated based on the original shared key stored in the private chain.

The calculation of the public parameters published by TA was 1 T_{mul} +1 T_h = 0.7761 ms, and the TA performed once for all vehicles. Therefore, when handling a large number of vehicles, the key generation for a single vehicle is computationally efficient, and the computational complexity associated with the TA's common parameters can be ignored. As a result, the computational cost for generating vehicle pseudonyms and keys is approximately 6 T_{mul} + T_{add} + 3T_h ≈ 4.6627 ms. Compared to the schemes proposed by Yang et al. [23], Liu et al. [24], and Shen et al. [22], the cost of generating pseudonyms and keys in this study has been reduced by 14.3%, 14.4%, and 83.8%, respectively.

Table 4. Comparison of Calculation Costs.

Scheme	Pseudonym and Partial Key Generation (ms)	V2R Message Signature (ms)	V2R Signature Verification (ms)	V2V Message Signature (ms)	V2V Message Verification (ms)
Bayat et al.'s [7]	$2T_{sm} + T_h \approx 1.5486$	$T_{sm} \approx 0.7741$	$3T_{bp} + T_{sm} + T_{mtp} \approx 22.3403$	-	-
Yang et al.'s [23]	$7T_{mul} + T_{add} + 6T_h \approx 5.4396$	$T_h \approx 0.0004$	$3T_{mul} + 4T_{add} + 2T_h \approx 2.3571$	-	-
Liu et al.'s [24]	$7T_{mul} + 2T_{add} + 2T_h \approx 5.4453$	$T_h + T_{mul} \approx 0.7761$	$3T_{mul} + 2T_{add} + 2T_h \approx 2.3425$	-	-
Shen et al.'s [22]	$3T_{bp} + 4T_{sm} + T_{pa} + 2T_{ep} + 4T_h \approx 28.7027$	$T_{bp} + T_{sm} + T_{ep} + T_h \approx 10.3724$	$2T_{bp} + 2T_{sm} + T_{pa} + T_{ep} + 2T_h \approx 17.5558$	-	-
This article's proposal	$6T_{mul} + T_{add} + 3T_h \approx 4.6627$	$T_h \approx 0.0004$	$2T_{mul} + T_{add} + 5T_h \approx 1.5607$	$T_h \approx 0.0004$	$5T_{mul} + T_{add} + 7T_h \approx 3.8886$

Cross-domain anonymous message authentication between vehicles and RSUs involves calculating the message signature $\delta = x_t H_2(PID_m, P_w, P_{vt}, M, AID_i, T_{\exp}) + w_m$ for the vehicle and the RSU verifying the signature $\delta P = H_2(PID_m, P_w, P_{vt}, M, AID_i, T_{\exp})P_{vt} + P_w$. If the vehicle is not in the same area as the RSU, the RSU needs to send a query request $H_3(P_{vt}, RSU_{id}, xu, T_{\exp}), RSU_{id}, P_{vt}, T_{\exp}$ to the TA in this region. The TA verifies the request, queries the temporary public key chain, and returns either a confirmation $H_3(P_{vt}, true, xu), true$, or an error $H_3(P_{vt}, false, xu), false$. The RSU then receives and verifies the response. Therefore, the cost of cross-domain message signing for vehicles is $T_h \approx 0.0004$ ms. Compared to the schemes of Liu et al. [24] and Shen et al. [22], the cost of generating pseudonyms and keys was reduced by 99.9% in both cases, whereas the computational complexity of Yang et al.'s [23] scheme remained similar. The maximum cost of verifying cross-domain signatures is $2T_{mul}$ + T_{add} + $5T_h \approx 1.5607$ ms. In comparison to the schemes developed by Yang et al. [23], Liu et al. [24], and Shen et al. [22], the cost of generating pseudonyms and keys was reduced by 33.8%, 33.4%, and 91.1%, respectively.

When authenticating cross-domain messages between vehicles, the vehicle calculates the $\delta_m = x_t H_2(PID_m, P_w, P_{vt}, M_m, AID_i, T_{\exp}) + w_m$. Upon receiving the message, the other vehicle verifies the equation $\delta_m P = H_2(PID_m, P_w, P_{vt}, M_m, AID_i, T_{\exp})P_{vt} + P_w$. If the equation holds and the two vehicles are not in the same area, the receiving vehicle calculates $PID_l = RID_l \oplus H_1(w_l P_{pub})$, $P_l = w_l P$, $H_4(P_{vt}, P_l, PID_l, T_{\exp}, x)$, and sends a query request to the TA in the current area. The TA then calculates $RID_l = PID_l \oplus H_1(sP_l)$, verifies if $H_4(P_{vt}, P_l, PID_l, T_{\exp}, x)$ holds true, and returns $H_3(P_{vt}, true, PID_l, x), true$ or $H_3(P_{vt}, false, PID_l, x), false$. The receiving vehicle then verifies the returned message. The cost of cross-domain message signing for vehicles is $T_h \approx 0.0004$ ms, whereas the maximum cost of verifying cross-domain signatures is $5T_{mul}$ + T_{add} + $7T_h \approx 3.8886$ ms. This scheme demonstrates significant advantages in computational complexity for generating pseudonyms and keys, as well as for message signing and signature verification. A comparative analysis of computational costs is shown in Figure 6.

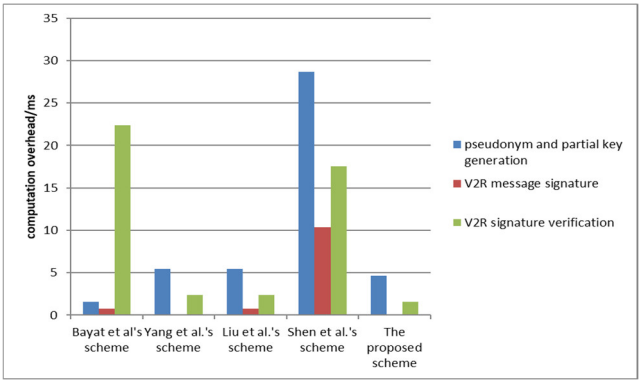

Figure 6. Calculation costs of different stages of each scheme [7,22–24].

6.2. Communication Overhead

To assess the communication overhead associated with pseudonym use, key generation, and authentication, the experiment set the real identity, AID and timestamp used in authentication to 4 bytes each, the hash length to 32 bytes, the element length in group G to 64 bytes, the length of elements in a bilinear group to 128 bytes, the length of message to L_m, and the length of other non-group elements to 32 bytes. A cost comparison of the communication schemes is presented in Table 5. In this study, pseudonyms are generated independently by the vehicle, resulting in no communication overhead for pseudonym generation. For key generation, the TA must publish the public key update parameter $(\sigma, P'_r, AID_i, T_{\exp})$. Therefore, the total communication length for the key generation update is 32 + 64 + 4 = 100 bytes.

Table 5. Comparison of Communication Costs.

Scheme	Pseudonym and Partial Key Generation (Byte)	V2R Message Signature (Byte)	V2R Signature Verification (Byte)	V2V Message Signature (Byte)	V2V Message Verification (Byte)	Overall Communication Overhead of V2R (Byte)	Overall Communication Overhead of V2V (Byte)
Bayat et al.'s [7]	356	$288 + L_m$	0	-	-	L_m + 644	-
Yang et al.'s [23]	144	$236 + L_m$	204	-	-	L_m + 584	-
Liu et al.'s [24]	416	$168 + L_m$	0	-	-	L_m + 584	-
Shen et al.'s [22]	292	$612 + L_m$	300	-	-	L_m + 1204	-
This article's proposal	100	$200 + L_m$	144	200	236	L_m + 444	L_m + 534

The signature sent by the vehicle in the vehicle-to-RSU (V2R) message signature is denoted as $(\delta, PID_m, P_w, P_{vt}, M, AID_i, T_{\exp})$. The length was calculated as 32 + 32 + 64 + 64 + 4 + 4 + L_m = 200 + L_m bytes.

During the V2R signature verification phase, if the vehicle and RSU are not in the same region, the RSU sends a query request $H_3(P_{vt}, RSU_{id}, xu, T_{\exp})$, RSU_{id}, P_{vt}, AID_i, $T_{\exp}$ to the TA in this region. The TA then replies with $H_3(P_{vt}, true, xu)$, $true$ or $H_3(P_{vt}, false, xu)$, $false$. The length of this communication is calculated as 32 + 4 + 64 + 4 + 32 + 4 + 4 = 144 bytes. Thus, the total cost of the V2R authentication was 100 + 200 + L_m + 144 = 444 + L_m bytes. The signature sent by the vehicle in the V2V (vehicle-to-vehicle) message signature is denoted as $(\delta_m, PID_m, P_w, P_{vt}, M_m, AID_i, T_{\exp})$. The length was calculated as 32 + 32 + 64 + 64 + 4 + 4 + L_m = 200 + L_m bytes. When verifying V2V signatures, if the vehicles and are not in the same area, the vehicle sends a query request $(H_4(P_{vt}, P_l, PID_l, x, T_{\exp}), PID_l, P_{vt}, P_l, AID_i, T_{\exp})$ to the TA

in the current area. The TA replies with either $H_3(P_{vt}, true, xu), true$ or $H_3(P_{vt}, false, xu), false$, with a length of 32 + 32 + 64 + 64 + 4 + 4 + 32 + 4 = 236 bytes.

This study demonstrates a significant advantage in reducing the total communication overhead of V2R authentication. Specifically, it achieves a reduction in communication overhead of approximately 23.9% compared to the schemes proposed by both Yang et al. [23] and Liu et al. [24], and a substantial reduction of 63.1% compared to the scheme proposed by Shen et al. [22].

To investigate other loads and overheads in communication, this paper also compares the number of information exchanges required during the message authentication process and the number of blockchain queries. Table 5 presents a comparison of the number of exchanges and blockchain queries for each scheme during the message authentication process. In this paper, when vehicles perform message authentication with RSU or between vehicles, the vehicle signs the message and sends it to the RSU or other vehicles. The RSU or other vehicles determine whether the sending vehicle is in the same area as themselves. If it is, they query the local consortium blockchain; if not, they query the global temporary public key blockchain. The local consortium blockchain or global temporary public key blockchain returns the query results to the RSU or receiving vehicle, requiring three communication exchanges and one blockchain query. Table 6 shows that the number of communication exchanges and blockchain queries in this paper's message authentication is the same as that in Yang and Shen's scheme, and more than Liu's scheme. However, Liu's scheme requires the blockchain for each generation of vehicle pseudonyms, while this paper's scheme does not. Therefore, the other communication overheads in this paper's message authentication are similar to mainstream schemes.

Table 6. Comparison of Other Communication Costs.

Scheme	Number of Message Authentication Communication Interactions	Number of Blockchain Queries During the Message Authentication Process
Bayat et al.'s [7]	2	-
Yang et al.'s [23]	3	1
Liu et al.'s [24]	1	1
Shen et al.'s [22]	3	1
This article's proposal	3	1

6.3. Other Performance Analysis

To analyze the impact of high-speed mobility of vehicles in VANETs on the scheme proposed in this paper, assuming the vehicle speed is 120 km/hour, approximately 0.33 km/s, the time overhead for message authentication in this paper is 0.0004 + 1.5607 = 1.5611 ms. During the authentication process, a blockchain query is required, which simply checks whether the temporary public key of the vehicle exists. The global temporary public key chain in this paper is stored by region, and the time consumed for a blockchain query based on region is approximately in the millisecond range. Adding other delays, a single message authentication will not exceed 1 s. The distance traveled by a vehicle within 1 s is 330 m. Within this diameter distance range, the communication delay between the vehicle and the RSU can be neglected. Therefore, the scheme proposed in this paper can be applied in high-speed mobile VANETs networks.

7. Conclusions

This scheme eliminates the need for certificates, thereby reducing the costs associated with certificate issuance and management. It ensures reliable authentication through the use of temporary public keys, and by updating parameters via public key issuance, each

node can independently update its temporary public key, making the implementation straightforward. The scheme not only achieves security attributes such as anonymity and unlinkability in authentication but also ensures high efficiency. It offers significant advantages in both computational and communication costs, making it well-suited for practical car-networking environments that require low authentication latency and robust large-scale privacy protection. The scheme proposed in this article can be further optimized for querying and updating public keys on the blockchain.

Author Contributions: The conceptualization of the study, developing the research methodology, and collecting the primary data, M.S. The data analysis, interpreting the results, and providing critical revisions to the manuscript, D.Z. The literature review Y.G. The design of some of the experimental procedures, X.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by in part by Natural Science Research Funding Project for Anhui Universities grant number 2022AH050386, in part by the National Natural Science Foundation of China grant number 61902140 and in part by the Natural Science Foundation of Anhui Higher Education Institutions grant number 2025AHGXZK20015. The APC was funded by 2022AH050386.

Data Availability Statement: Data is contained within the article.

Acknowledgments: This work was supported in part by Natural Science Research Funding Project for Anhui Universities under Grant 2022AH050386, in part by the National Natural Science Foundation of China under Grant No. 61902140 and in part by the Natural Science Foundation of Anhui Higher Education Institutions under Grant No. 2025AHGXZK20015.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476. [CrossRef]
2. Wang, S.; Yao, N. LIAP: A local identity-based anonymous message authentication protocol in VANETs. *Comput. Commun.* **2017**, *112*, 154–164. [CrossRef]
3. Chen, C.L.; Chen, Y.X.; Lee, C.F.; Deng, Y.Y.; Chen, C.H. An efficient and secure key agreement protocol for sharing emergency events in VANET systems. *IEEE Access* **2019**, *7*, 148472–148484. [CrossRef]
4. Xie, Y.; Wu, L.; Shen, J.; Alelaiwi, A. EIAS-CP: New efficient identity-based authentication scheme with conditional privacy-preserving for VANETs. *Telecommun. Syst.* **2017**, *65*, 229–240. [CrossRef]
5. Zhong, H.; Wen, J.; Cui, J.; Zhang, S. Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET. *Tsinghua Sci. Technol.* **2016**, *21*, 620–629. [CrossRef]
6. Deng, L.; Shao, J.; Hu, Z. Identity based two-party authenticated key agreement scheme for vehicular ad hoc networks. *Peer-Peer Netw. Appl.* **2021**, *14*, 2236–2247. [CrossRef]
7. Bayat, M.; Pournaghi, M.; Rahimi, M.; Barmshoory, M. NERA: A new and efficient RSU based authentication scheme for VANETs. *Wirel. Netw.* **2020**, *26*, 3083–3098. [CrossRef]
8. Alazzawi, M.A.; Lu, H.; Yassin, A.A.; Chen, K. Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network. *IEEE Access* **2019**, *7*, 71424–71435. [CrossRef]
9. Verchyk, D.; Sepúlveda, J. A practical study of post-quantum enhanced identity-based encryption. *Microprocess. Microsyst.* **2023**, *99*, 104828. [CrossRef]
10. Paliwal, S.; Cherukuri, A.K.; Gao, X.Z. Dynamic private modulus based password conditional privacy preserving authentication and key-agreement protocol for VANET. *Wirel. Pers. Commun.* **2022**, *123*, 2061–2088. [CrossRef]
11. Li, X.; Liu, T.; Obaidat, M.S.; Wu, F.; Vijayakumar, P.; Kumar, N. A lightweight privacy-preserving authentication protocol for VANETs. *IEEE Syst. J.* **2020**, *14*, 3547–3557. [CrossRef]
12. Shamshad, S.; Saleem, M.A.; Obaidat, M.S.; Shamshad, U.; Mahmood, K.; Ayub, M.F. On the security of a lightweight privacy-preserving authentication protocol for VANETs. In *Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*; IEEE: Piscataway, NJ, USA, 2021.
13. Alfadhli, S.A.; Lu, S.; Fatani, A.; Al-Fedhly, H.; Ince, M. SD2PA: A fully safe driving and privacy-preserving authentication scheme for VANETs. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 38. [CrossRef]

14. Lee, J.; Yu, S.; Kim, M.; Park, Y.; Lee, S.; Chung, B. Secure key agreement and authentication protocol for message confirmation in vehicular cloud computing. *Appl. Sci.* **2020**, *10*, 6268. [CrossRef]
15. Alfadhli, S.A.; Lu, S.; Chen, K.; Sebai, M. MFSPV: A multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs. *IEEE Access* **2020**, *8*, 142858–1428741. [CrossRef]
16. Lv, S.; Liu, Y. PLVA: Privacy-preserving and lightweight V2I authentication protocol. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6633–6639. [CrossRef]
17. Wang, C.; Shen, J.; Lai, J.F.; Liu, J. B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs. *IEEE Trans. Emerg. Top. Comput.* **2020**, *9*, 1386–1396. [CrossRef]
18. Maria, A.; Rajasekaran, A.S.; Al-Turjman, F.; Altrjman, C.; Mostarda, L. BAIV: An efficient blockchain-based anonymous authentication and integrity preservation scheme for secure communication in VANETs. *Electronics* **2022**, *11*, 488. [CrossRef]
19. Son, S.; Lee, J.; Park, Y.; Park, Y.; Das, A.K. Design of blockchain-based lightweight v2i handover authentication protocol for VANET. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 1346–1358. [CrossRef]
20. Yao, Y.; Chang, X.; Mišić, J.; Mišić, V.B.; Li, L. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. *IEEE Internet Things J.* **2019**, *6*, 3775–3784. [CrossRef]
21. Wazid, M.; Das, A.K.; Kumar, N.; Odelu, V.; Reddy, A.G.; Park, K.; Park, Y. Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. *IEEE Access* **2017**, *5*, 14966–14980. [CrossRef]
22. Shen, M.; Liu, H.; Zhu, L.; Xu, K.; Yu, H.; Du, X.; Guizani, M. Blockchain-assisted secure device authentication for cross-domain industrial IoT. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 942–954. [CrossRef]
23. Yang, Y.; Wei, L.; Wu, J.; Long, C.; Li, B. A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network. *IEEE Internet Things J.* **2021**, *9*, 8078–8090. [CrossRef]
24. Liu, X.; Zhong, Q.; Xia, Y. Efficient authentication scheme for cross-trust domain of IoV based on double-layer shard blockchain. *J. Commun.* **2023**, *44*, 213–223.
25. Dwivedi, S.K.; Amin, R.; Vollala, S.; Khan, M.K. B-HAS: Blockchain-assisted efficient handover authentication and secure communication protocol in VANETs. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 3491–3504. [CrossRef]
26. Pointcheval, D.; Stern, J. Security Proofs for Signature Schemes. In *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques Saragossa, Spain, 12–16 May 1996*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1996; Volume 1070, pp. 387–404.
27. Yadulla, A.R.; Yenugula, M.; Kasula, V.K.; Konda, B.; Addula, S.R.; Rakki, S.B. A time-aware LSTM model for detecting criminal activities in blockchain transactions. *Int. J. Commun. Inf. Technol.* **2023**, *4*, 33–39. [CrossRef]