electronics

Article

BPA: A Novel Blockchain-Based Privacy-Preserving Authentication Scheme for the Internet of Vehicles

Jie Li [1,2], Yuanyuan Lin [1], Yibing Li [3], Yan Zhuang [1] and Yangjie Cao [1,*]

[1] School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450001, China; lijie@cs.sjtu.edu.cn (J.L.)
[2] Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China
[3] School of Computer and Artificial Intelligence, Zhengzhou University, Zhengzhou 450001, China
* Correspondence: caoyj@zzu.edu.cn

Abstract: The Internet of Vehicles (IoV) connects an isolated individual on the road to share information, which can improve traffic efficiency. However, the promotion of information sharing brings the critical security issues of identity authentication, followed by privacy protection issues in the authentication process in the IoV. In this study, we designed a blockchain-based conditional privacy-preserving authentication scheme for the IoV (BPA). Our scheme implements zero-knowledge proof (ZKP) to verify the identities of vehicles, which moves the authentication process down to the Roadside Units (RSUs) and achieves decentralized authentication at the edge nodes. Moreover, blockchain technology is utilized to synchronize a consistent ledger across all RSUs for recording and disseminating vehicle authentication states, which enhances the overall authentication process efficiency. We provide a theoretical analysis asserting that the BPA ensures enhanced security and effectively protects the privacy of all participating vehicles. Experimental evaluations confirm that our scheme outperforms existing solutions in terms of the computational and communication overhead.

Keywords: internet of vehicles (IoV); anonymous authentication; blockchain; privacy preservation

Citation: Li, J.; Lin, Y.; Li, Y.; Zhuang, Y.; Cao, Y. BPA: A Novel Blockchain-Based Privacy-Preserving Authentication Scheme for the Internet of Vehicles. *Electronics* **2024**, *13*, 1901. https://doi.org/10.3390/electronics13101901

Academic Editor: Fabio Grandi

Received: 22 April 2024
Revised: 2 May 2024
Accepted: 3 May 2024
Published: 13 May 2024

1. Introduction

With the rapid development of intelligent technology and urbanization, intelligent transportation has attracted widespread attention in the academic and industrial communities [1,2]. As an essential component of intelligent transportation systems, the Internet of Vehicles (IoV) can realize intelligent traffic management and dynamic information services in modern transportation scenarios, bringing great convenience and comfortable driving experiences to people [3]. Figure 1 shows a typical architecture of the IoV, mainly including a TA (Trusted Authority), RSUs (Roadside Unit), and vehicles. The TA is a trusted server able to store relevant vehicle information and manage it effectively, which is usually played by the government in reality. An RSU is road infrastructure fixed on the roadside with computing and communication capabilities that can provide services to vehicles [4]. When the vehicle is within the communication range of an RSU, it can communicate with the RSU to transmit real-time road data including position and speed. After receiving the data transmitted by the vehicle, the RSU is able to analyze the data to evaluate the current road condition. Based on the analysis results, RSUs then disseminate road condition information back to the vehicles, aiding them in route planning. However, the accuracy of the information provided by the RSU is highly dependent on the data uploaded by the vehicle [5]. Malicious vehicles transmitting falsified data can skew RSU analyses, leading to the dissemination of incorrect road condition information and thereby posing significant risks to the safety of legitimate drivers and overall road safety [6].

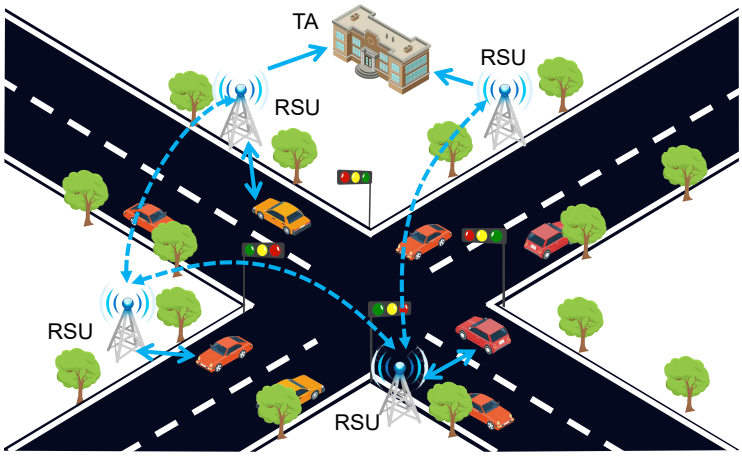

Figure 1. Typical architecture of IoV.

Authentication acts as a critical measure to address the aforementioned issues by ensuring the authenticity and legitimacy of vehicle identities within the IoV. However, the authentication data of vehicles may contain privacy details, such as location, which could be exploited by malicious attackers. Malicious attackers might track the activities of vehicles using this sensitive information to deduce their actual identities, thereby compromising vehicle security [7]. Consequently, it is imperative that vehicles maintain anonymity throughout the authentication process to prevent the disclosure of private details [8]. While absolute anonymity safeguards privacy, it can complicate vehicle identity management. Specifically, it can lead to issues such as the propagation of malicious messages without the ability to trace the actual identities of the culprits [9,10]. Therefore, conditional anonymity becomes crucial in vehicle authentication. In other words, the true identities of vehicles are not revealed to the RSU throughout the authentication process, but the TA can trace and reveal it if necessary (in an investigation or through the presentation of a court order) [11,12].

Most existing authentication schemes employ a TA to verify the identities of vehicles, with the RSU serving as an intermediate node that relays authentication requests from the vehicles to the TA [5]. Consequently, the TA must efficiently conduct vehicle identity verification and key agreement. However, the high speeds of the vehicles pose challenges for the TA to accomplish these tasks quickly. When a substantial number of vehicles request authentication within a brief period, it is susceptible to the communication and computing resource bottlenecks of the TA, hindering the completion of the verification within the specified time. Simultaneously, RSUs only handle message forwarding, contributing to increased communication overhead in the authentication process and leading to resource wastage.

Zero-knowledge proofs (ZKPs) allow the prover to demonstrate to the verifier the correctness of an assertion (meeting the specified requirements) without providing any useful information (any private data) to the verifier [13]. ZPK can be adopted to for authentication without third-party involvement. In the ZKP process, the prover generates proof based on system parameters published by the trusted setup and sends it to the verifier for verification, eliminating the need for third-party involvement. However, this approach may lead to absolute anonymity in vehicle authentication. Traditional ZKP, such as zk-SNARK and zk-STARKs, may introduce substantial communication and computational overhead [14].

In addition, as a vehicle will traverse multiple RSUs during its journey, it is required to undergo authentication processes with each subsequent RSU they encounter. Conducting authentication at every instance can lead to redundant computations, resulting in unnecessary overhead and decreased efficiency. Therefore, it is necessary to mitigate the computational redundancy during the re-authentication phase, aiming to alleviate the burden on the vehicle and minimize network delays. A feasible measure to enhance efficiency is sharing the vehicle authentication status with subsequent RSUs. When a

vehicle is driven to other RSUs, it does not need to be verified again, thus improving the efficiency. Blockchain is a decentralized, immutable, and traceable technology that can share information between peers, and can ensure that the information is not tampered with, so that the vehicle's authentication status can be correctly shared with other RSUs. And because of the traceability of blockchain, when a malicious vehicle sends false information, it can be traced. It is appropriate to share the authentication status of the vehicle through blockchain [5].

In this paper, we propose a novel blockchain-based privacy-preserving authentication scheme (BPA) that utilizes blockchain and ZPK to safeguard privacy and improve efficiency during the authentication process. Our scheme moves the authentication process down to the RSU and optimize the re-authentication phase. The main contributions of our scheme are as follows:

- We developed a blockchain-based privacy-preserving authentication scheme (BPA) to verify the legitimacy of vehicle identities. Our scheme comprises five phases: system initialization, registration, authentication, re-authentication, and revocation, which are cover the whole life cycle of the management and usage of identities in the IoV.
- Our scheme utilizes ZKP to transfer the authenticated computing load to the RSU, eliminating communication latency to some extent. In the re-authentication process after the initial authentication process, we utilize blockchain to share vehicle authentication processes among RSUs, avoiding the redundant computations by sharing and maintaining the trust key of each vehicle among the RSUs, reducing the computational overhead of the vehicles.
- We conducted a rigorous security analysis to prove the security and integrity of our scheme, which is strong enough to protect the privacy and secrecy of vehicle identities. Compared with other schemes, our scheme has more advantages.

We organized the remainder of this paper as follows. In Section 2, we discuss the existing privacy authentication schemes related to the IoV, and in Section 3, we define the system model and attack model and discuss background knowledge. Then, we describe our proposed scheme in detail in Section 4. In Section 5, we analyze the security of our scheme. In Section 6, we compare the performance of our scheme with those of existing schemes. And in Section 7, Open Challenges and Future Research Directions are described. Finally, we conclude this paper in Section 8.

2. Related Work

Many schemes have been proposed for vehicle privacy protection in IoV, which can be broadly divided into Public Key Infrastructure (PKI)-based, ID-based, certificateless, and blockchain-based.

PKI-based schemes commonly employ anonymous certificates to protect vehicle privacy, as demonstrated in the approach introduced by Raya and Hubaux [15]. However, this scheme requires vehicles to preload certificates, requiring substantial computing and communication resources. Qiu et al. [16] designed a PKI-based authentication scheme using Recurrent Neural Networks (RNNs) that predict the future routes and locations of vehicles. By pre-assigning keys to vehicles in their respective areas, this approach eliminates the need for key update requests. Nevertheless, this scheme incurs a significant computational overhead. Heng et al. [17] designed a scheme utilizing accumulators to maintain a certificate revocation list, which provides a revocation phase for vehicles. However, this scheme necessitates frequent certificate renewals to ensure the vehicles' privacy.

To address the shortcomings existing in PKI-based schemes, researchers have proposed ID-based schemes that mainly utilize pseudonym methods for authentication. The scheme presented by He et al. [18] involves storing the secret key of the TA in the vehicle's tamper-proof device. This key is then employed to generate authentication information when the vehicle requires authentication. Unfortunately, this scheme falls short in providing a relevant vehicle revocation mechanism. Ma et al. [19] designed an authentication scheme utilizing XOR and Elliptic Curve Cryptography (ECC) to achieve multi-party authentication

among vehicles, fog nodes, and cloud servers. However, Awais et al. [20] pointed out that the scheme is susceptible to impersonation attacks by vehicle users and does not provide anonymity for vehicles. Additionally, Vasudev [21] proposed an authentication method for vehicles using XOR and hash operations, but this approach is centralized, potentially leading to computational bottlenecks.

In the certificateless authentication scheme, the private key of the user is composed of two parts: one part is generated by the KGC based on the identity information, and the other part is generated by the user themselves, which circumvents the issue of key escrow. Chen et al. [22] designed a certificateless authentication scheme. However, it was pointed out by Xu et al. [23] that the scheme has security vulnerabilities and is unable to resist public key substitution attacks. Furthermore, in the scheme of Xu [23], vehicles are required to send pseudonyms to the RSU, which fails to provide unlinkability. Kamil [24] designed an aggregate signature scheme. However, Zhao et al. [25] discovered that their scheme has security issues and is unable to resist forgery attacks, subsequently proposing an improved certificateless authentication scheme. Han et al. [26] introduced a certificateless aggregate authentication scheme based on Elliptic Curve Cryptography (ECC). Yet, Zheng et al. [27] found that this scheme could not ensure the security of the master key, as attackers could infer the master key from the keys generated for vehicles by the KGC.

ZKP allows the prover to generate proofs without revealing any relevant information, while the verifier verifies the proof of the prover. In recent years, some researchers have employed ZKP in the domain of privacy-preserving authentication in the IoV. To the best of our knowledge, Amar et al. [28] were the first to apply ZKP for privacy-preserving authentication in the IoV. They presented a ZKP-based authentication using quadratic residuosity and realized the anonymity of vehicles through the bidirectional ZKP cryptographic protocol. However, the scheme is based on interactive ZKP, which requires multiple interactions between the RSU and the vehicle, and it requires pre-shared secret keys. Ning et al. [29] adopted ZKP based on the Fujisaki–Okamoto (FO) Commitment and Elliptic Curve Cryptography (ECC) to achieve vehicle authentication, but in the authentication phase, the authentication server needs to send the relevant information about the vehicle to the TA to verify the identity of the vehicle. Varma et al. [30] used ZK-SNARK to authenticate the vehicle, which effectively protects the user privacy of the vehicle. But the bilinear mapping used in this scheme may bring large computational overhead.

Blockchain enables participants to keep a secure and traceable ledger. Xu et al. [5] proposed a blockchain-based scheme utilizing multiple Trust Authorities (TAs) for maintaining the blockchain. During authentication, vehicles send their information via Road Side Units (RSUs) to the TAs, who authenticate the vehicles. However, using multiple TAs, although distributing the computational load, introduces communication delays due to the RSU relay. Meng et al. [31] developed a similar scheme, also potentially increasing the delay with RSU-based transmission. Wang et al. [32] used blockchain to assess vehicle trustworthiness, employing bilinear mapping for authentication, but they overlooked vehicle traceability. Xie et al. [33] enhanced the authentication efficiency by storing information on the blockchain, requiring pseudonym updates through TAs. B-DSPA [34] identifies security flaws in Zhang's [35] scheme, allowing secret parameters and vehicle trajectories to be inferred. Additionally, Tao et al. [34] designed a privacy-preserving scheme with smart contracts for accident tracking and forensics, enhancing safety.

3. System Overview

3.1. System Model

The proposed scheme covers the whole life cycle of vehicle authentication, which consists of four phases: registration, authentication, re-authentication, and revocation. When a vehicle drives on the road, it traverses the coverage of multiple RSUs, requiring continuous authentication with these RSUs. An RSU assumes the responsibility of authenticating and exchanging information with vehicles as they enter its coverage area. The proposed model

is illustrated in Figure 2, which consists of four parts: the TA, RSU, vehicle, and blockchain. A detailed description of each part is as follows:

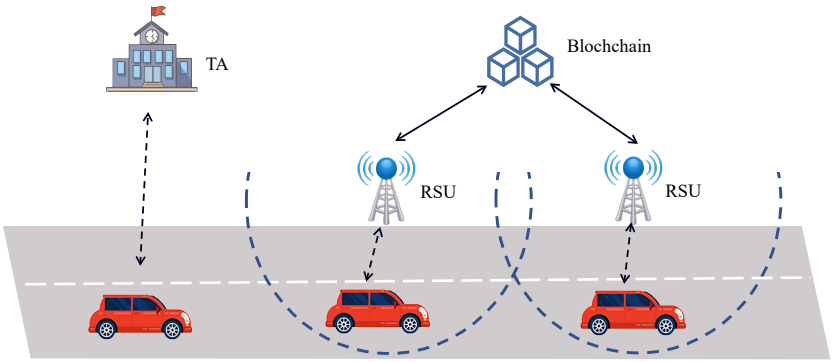

Figure 2. The IoV authentication architecture of the BPA.

- TA: The TA is responsible for generating the system's public parameters and deploying the RSU. Additionally, the TA distributes the keys to corresponding users and reveals the genuine identity of the vehicle. In our proposed scheme, the TA is deemed a trusted entity, which is usually played by the government in reality. It is assumed to possess significant computational resources and is expected to operate without colluding with other entities.
- RSU: Deployed at the roadside, all RSUs collectively maintain a consortium blockchain. When a vehicle enters its communication range, the RSU uploads the vehicle's authentication information to the blockchain, and subsequent RSUs can authenticate the vehicle based on the data recorded on the blockchain.
- Vehicle: Equipped with an OBU (on-board Unit) possessing computational power, vehicles need to register with a TA before accessing the IoV. Following registration, vehicles obtain relevant traffic information and services by authenticating with the RSU after entering the RSU's communication range.
- Blockchain: All RSUs collaboratively maintain a consortium blockchain utilizing the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. When the vehicle accesses the IoV for the first time, it uses the key issued by the TA to authenticate. The RSU uploads the vehicle's authentication token to the blockchain. When the vehicle travels to the next RSU, it is authenticated based on the information uploaded to the blockchain.

3.2. Attack Model

In our scheme, the TA assumes the role of a trusted third party, performed by a government department in reality, ensuring the non-disclosure of user data and resilience against potential threats from malicious participants. But as RSUs are deployed on the side of the road, they are vulnerable to adversaries that want to obtain their records and deduce the true identity of vehicles. Moreover, malicious vehicles may attempt to obtain keys used for authentication by collecting and eavesdropping on data from legitimate vehicles, deduce the true identity of a vehicle, conduct replay attacks using outdated authentication messages, or falsify parameters to simulate legitimate vehicles during the authentication process. At the same time, two or more malicious vehicles may collude to obtain the TA's private key. The authentication scheme we designed can satisfy the following security objectives:

- Anonymity and Unlinkability: During the authentication process between vehicles and RSUs, the identity of the vehicle is confidential, and the RSUs cannot obtain it. Even if RSUs or adversaries acquire the vehicle's authentication information, they cannot track the vehicle's activities or infer the vehicle's real identity from this information.

- Traceability: If a vehicle engages in illegal activities, the TA (Trusted Authority) can trace and reveal the vehicle's real identity information.
- Forward Secrecy: Even if attackers possess the keys for the current session, they cannot obtain information from previous sessions.
- Resistance to Replay Attacks: Attackers cannot pass identity verification by sending expired authentication information of the vehicle.
- Collusion Attack: Multiple attackers cannot deduce the TA's key from the registration or authentication information.
- Impersonation Attack: Even if attackers can obtain a vehicle's authentication information, they cannot simulate legitimate authentication information to authenticate.

3.3. Elliptic Curve Cryptography (ECC)

ECC is a type of asymmetric encryption algorithm based on the mathematical theory of elliptic curves. Points on the elliptic curve E defined over the finite field F_q satisfy the following:

$$y^2 = x^3 + ax + b \ (\ mod\ p\ ), 4a^3 + 27b^2 \neq 0 \ (\ mod\ p\ ), a, b \subseteq Z_q^*$$

Let G be the set of points on the elliptic curve, which is an additive cyclic group with order n and generator P under the point addition operation. The mathematical computational problems of ECC are as follows:

- Elliptic curve discrete logarithm (ECDL) problem: Select the points Q and P that satisfy $Q = a \cdot P$ on the elliptic curve E (P is the generator of $E, a \in Z_q^*$); it is hard to find a when Q and P are given.
- Elliptic curve computational Diffie–Hellman assumption (ECCDH) problem: Select the points V, Q, and P that satisfy $Q = a \cdot P$ and $V = b \cdot P$ on the elliptic curve E (P is the generator of $E, a, b \in Z_q^*$); it is hard to compute $ab \cdot P$ when Q, V, and P are given.
- Elliptic curve decisional Diffie–Hellman assumption (ECDDH) problem: Select the points S, V, Q, and P that satisfy $Q = a \cdot P, V = b \cdot P$, and $S = c \cdot P$ on the elliptic curve E (P is the generator of $E, a, b, c \in Z_q^*$); it is hard to determine whether $c \cdot P \stackrel{?}{=} ab \cdot P$ when S, V, Q, and P are given.

3.4. Zero-Knowledge Proof

The following is a zero-knowledge proof that relies on ECC $Q = a \cdot P$:

Let G be a cyclic group on an elliptic curve, with P as the generator and q as order. H is a one-way hash function. Choose a random number $a \in Z_q^*$ and compute $Q = a \cdot P$ in group G.

Prove: The prover that owns the secret value a calculates $Q = a \cdot P$ in group G. Then, the prover randomly chooses a random number n and calculates $N = n \cdot P$. The proof generated is as follows: $C = H(Q \parallel N)$ and $s = n + aC(mod\ p)$. Then, the prover sends the proof (C, s, Q) to the verifier.

Verify: The verifier calculates $N' = s \cdot P - QC$ and verifies $C \stackrel{?}{=} H(Q \parallel N')$. If the equation holds true, then the verification is successful.

4. Our Scheme

In this section, we will describe the proposed authentication scheme in detail, which consists of five phases: system initialization, registration, authentication, re-authentication, and tracing and revocation. Table 1 catalogs the notations of the proposed scheme.

The TA first publishes the system parameters for the system. Before the vehicle establishes its initial connection to the RSU, it is required to undergo registration with thee TA. Then, the registered vehicle conducts the initial authentication with an RSU, gaining access to services securely. Following successful initial authentication, the RSU will upload the verification token to the blockchain. Given the high-speed motion of vehicles and the limited coverage range of RSUs, vehicles will traverse multiple RSUs during their

journey. When a vehicle enters the communication range of the next RSU, this RSU utilizes the vehicle token previously uploaded to the blockchain by the former RSU for quick authentication and correspondence with the vehicle. In instances of vehicular misbehavior, the RSU can upload a revocation transaction to the blockchain indicating that the vehicle is illegal. The TA can reveal the true identity of the vehicle based on the information previously registered. The detailed description of each phase is as follow.

Table 1. Notations and their meanings.

Notation	Meaning
V_i	i-th vehicle
RSU_j, RSU_k	j-th and k-th RSU
VID_i	i-th vehicle's id
G	additive cyclic group
P	generator of G
sk	private key of TA
PK	public key of TA
s_j, s_k	private keys of RSU_j and RSU_k
P_j, P_k	public keys of RSU_j and RSU_k
T_i	timestamp (i = 1, 2, 3, ...)
$H()$	hash function
$\oplus$	exclusive OR operation
$\|\|$	concatenation operation
δ	maximum transmission delay

4.1. System Initialization

The TA initializes the system, generating public parameters and the private key of the TA, which will be used in subsequent phases:

- The TA generates an additive group G on a elliptic curve E with prime order q and generator P.
- The TA random chooses $s \in Z_q^*$ as it's private key sk and calculates $PK = sk \cdot P$ as a public key. Then, the TA constructs a secure one-way hash function $H_i : \{0,1\} \longrightarrow Z_q^*$, where $i = 1, 2$.
- The TA randomly chooses $s_j \in Z_q^*$ as a private key and computes $P_j = s_j \cdot P$ as a public key for RSU_j. The TA sends $\{s_j, P_j\}$ to RSU_j, where the public key is public, and the private key is private to the RSU_j.
- The TA sets the visibility of the parameters, where $params = \{G, P, PK, q, H_i\}$ is public, and the private key sk is private.

4.2. Registration

Before the authentication phase, the vehicle is required to register with the TA to obtain its private key and assert its legitimacy, as detailed in Figure 3:

- The vehicle V_i encrypts its own vehicle VID_i (which is only known to the vehicle itself) with the public key of the TA by computing $P_{VID_i} = VID_i \cdot P$ and $C_{VID_i} = VID_i + VID_i \cdot PK$. Then, V_i sends $\{P_{VID_i}, C_{VID_i}\}$ to TA.
- The TA computes $VID_i = C_{VID_i} - P_{VID_i} \cdot sk$ to obtain the VID_i.
- The TA randomly chooses $r \in Z_q^*$ and computes $R = r \cdot P$, $C_1 = H_1(R \parallel PK)$ and $\sigma_1 = r + skC_1 + VID_iC_1$ and records $\{R, C_1, VID_i\}$ in its database. Then, the TA sends $\{R, \sigma_1\}$ to V_i.
- V_i computes $C_1 = H_1(R \parallel PK)$. Then, it verifies $\sigma_1 \cdot P \stackrel{?}{=} R + PK \cdot C_1 + VID_i \cdot C_1$. If the verification is successful, V_i computes $\sigma_2 = \sigma_1 - VID_iC_1 = r + skC_1$ as its partial private key for initial authentication.

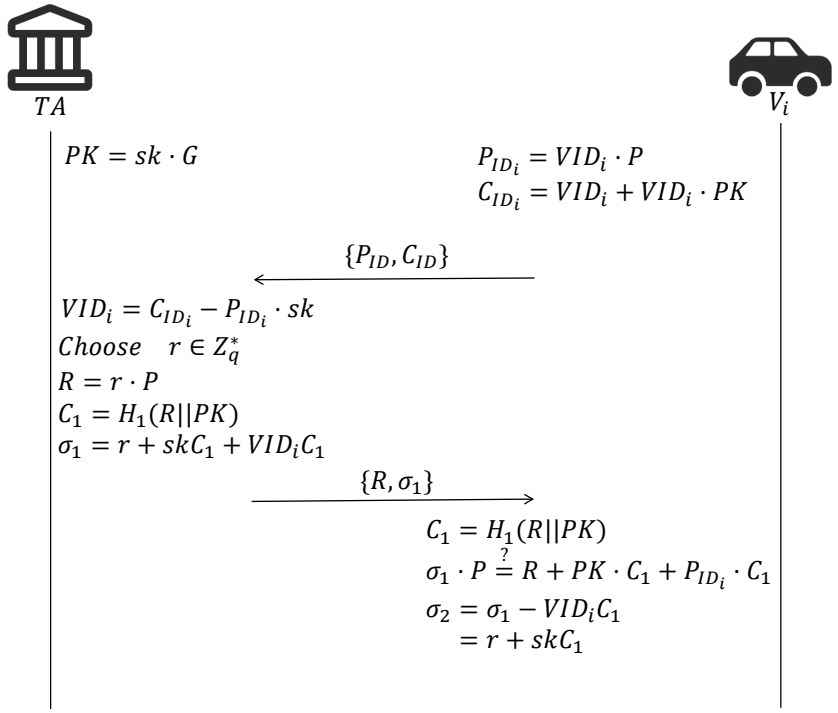

Figure 3. Registration phase.

4.3. Initial Authentication

V_i can be authenticated with the RSU_j when it drives within its coverage after completing the registration phase. The initial authentication phase is shown in Figure 4.

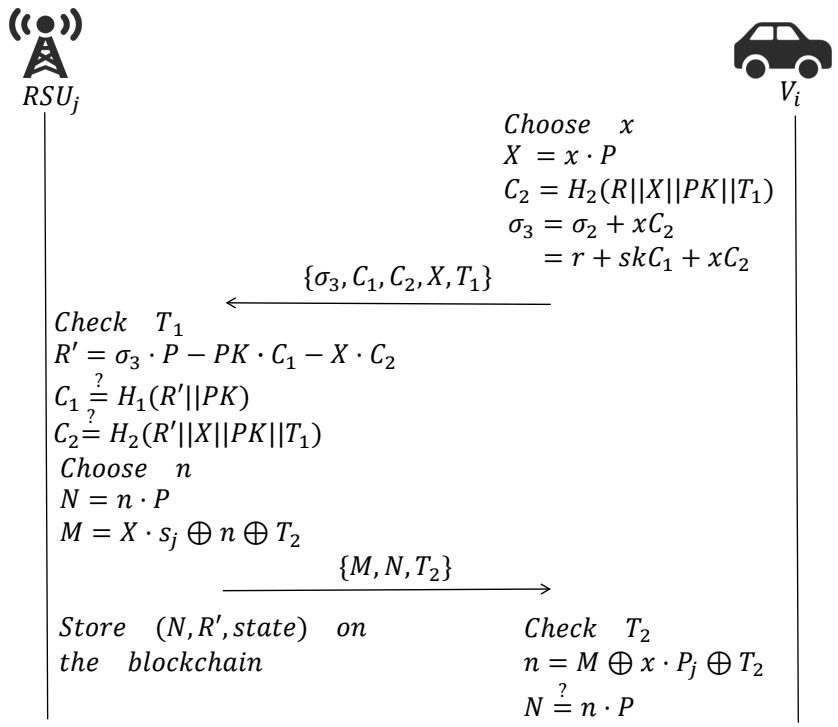

Figure 4. Initial authentication phase.

The phase is as follows:

- V_i first generates a random number $x \in Z_q^*$ and computes $X = x \cdot P$, $C_2 = H_2(R \parallel X \parallel PK \parallel T_1)$ and $\sigma_3 = (\sigma_2 + xC_2) \mod q = (r + skC_1 + xC_2) \mod q$. Then, V_i transmits $\{\sigma_3, C_1, C_2, X, T_1\}$ to RSU_j for authentication.
- After receiving the authentication request and parameters sent by V_i, RSU_j first checks T_1. If $T_2 - T_1 \leq \delta$, the RSU_j continues to authenticate; otherwise, it terminates this authentication. Note that T_2 is the current timestamp and δ is a predefined maximum transmission delay.
- RSU_j computes $R' = \sigma_3 \cdot P - PK \cdot C_1 - X \cdot C_2$ and verifies $C_1 \stackrel{?}{=} H_1(R' \parallel PK)$ and $C_2 \stackrel{?}{=} H_2(R' \parallel X \parallel PK \parallel T_1)$. If the verification is successful, V_i is considered to be legal; otherwise, the authentication fails.
- After a successful authentication, RSU_j randomly selects $n \in z_q^*$ and calculates $N = n \cdot P$ and $X \cdot s_j$, where $X \cdot s_j$ is used as the session negotiation key between RSU_j and V_i for later communication, and n is the parameter to be used by V_i in the next authentication. Then, RSU_j computes $M = X \cdot s_j \oplus n \oplus T_2$ and transmits $\{M, N, T_2\}$ to V_i. $X \cdot s_j$ is used as the negotiation key for the RSU_j between RSU_j and V_i.
- RSU_j uploads $(N, R', state)$ to the blockchain, where R' is equal to the R sent by the TA to V_i. The parameter *state* refers to the current state of the vehicle, such as legal and illegal. Then, the ledger will be updated among the RSUs through the PBFT consensus algorithm.
- After V_i receives the parameters sent back by RSU_j, it also checks T_2 first and then calculates $n = M \oplus x \cdot P_j \oplus T_2$ and verifies $N \stackrel{?}{=} n \cdot P$. $x \cdot P_j$ is used as the negotiation key for V_i. If this equation holds, it indicates that the parameters have not been tampered with during the transmission process, and the parameter n can be used in the next authentication.

4.4. Re-Authentication

After the initial authentication phase, the vehicle enters the re-authentication phase when it enters following RSU, where it authenticates using the parameters sent by the previous RSU. The details are shown in Figure 5.

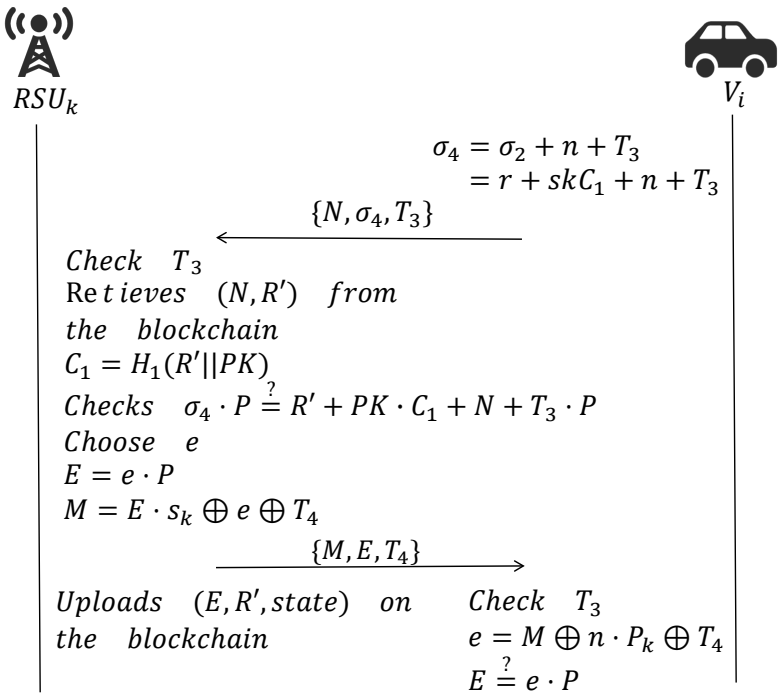

Figure 5. Re-authentication phase.

The phase is as follows:

- The vehicle V_i uses the parameter n sent by RSU_j after the last authentication to calculate $\sigma_4 = (\sigma_2 + n + T_3) \mod q = (r + s + n + T_3) \mod q$ and send the $\{N, \sigma_4, T_3\}$ to RSU_k.
- RSU_k checks T_3 and retrieves the transaction $(N, R', state)$ from the blockchain. Thereafter, RSU_k computes $C_1 = H_1(R' \parallel PK)$ and verifies $\sigma_4 \cdot P \stackrel{?}{=} R' + PK + N + T_3 \cdot P$.
- If the verification is successful, RSU_k randomly chooses $e \in z_q^*$ and computes $E = e \cdot P, M = E \cdot s_k \oplus e \oplus T_4$. Then, RSU_k transmits $\{M, E, T_4\}$ to V_i.
- The RSU_k uploads $(E, R', state)$ to the blockchain; note that R' is consistent with the R' uploaded by the previous RSU.
- V_i checks T_4 first and then calculates $e = M \oplus n \cdot P_j \oplus T_4$ and verifies $E \stackrel{?}{=} e \cdot P$.

4.5. Tracing and Revocation

If a malicious vehicle in the IoV transmits false messages or has illegal behavior and is detected by an RSU, the RSU will upload a revocation transaction to the blockchain, marking the vehicle as illegitimate. As a result, subsequent attempts to authenticate the vehicle will fail. At the same time, based on the authentication information sent by the vehicle, the record R can be retrieved from the blockchain. This record is subsequently forwarded to the TA, allowing TA to reveal the genuine identity of the vehicle by referencing the record of the vehicle from the registration phase.

5. Security Analysis

5.1. Correctness

When the RSU receives the authentication message from the vehicle, it can verify the correctness using the following equation:

$$\begin{aligned} C_1 &= H_1(R^{'} \parallel PK) \\ &= H_1((\sigma_3 \cdot P - PK \cdot C_1 - X \cdot C_2) \parallel X \parallel PK \parallel T_1) \\ &= H_1(((r + skC_1 + xC_2) \cdot P - PK \cdot C_1 - X \cdot C_2) \parallel X \parallel PK \parallel T_1) \\ &= H_1(R \parallel PK) \end{aligned} \tag{1}$$

$$\begin{aligned} C_2 &= H_2(R^{'} \parallel X \parallel PK \parallel T_1) \\ &= H_2((\sigma_3 \cdot P - PK \cdot C_1 - X \cdot C_2) \parallel X \parallel PK \parallel T_1) \\ &= H_2(((r + skC_1 + xC_2) \cdot P - PK \cdot C_1 - X \cdot C_2) \parallel X \parallel PK \parallel T_1) \\ &= H_2(R \parallel X \parallel PK \parallel T_1) \end{aligned} \tag{2}$$

5.2. Formal Security Analysis

In this section, we use a random oracle model (ROM) similar to Wang et al.'s [36] to prove that the proposed scheme is essentially unforgeable against type-I attacker $\mathcal{A}_1$ and type-II attacker $\mathcal{A}_2$ under the ROM.

Security Definition 1: As the ECDLP in elliptic curves is difficult, we propose a scheme that is essentially unforgeable against a *type-I* adversary in the ROM.

Type-I Attacker Capabilities: $\mathcal{A}_1$ indicates an external adversary that can obtain and replace the vehicle's public key but cannot obtain the system vehicle private key. It needs to comply with the queries defined in the following proof phase.

proof: To prove *Security Definition 1*, we simulate a challenger $\mathcal{C}$ that supports $\mathcal{A}_1$ to break our scheme and solve the ECDLP assumption that finds the private key sk of $PK = sk \cdot P$.

- Setup(): When $\mathcal{A}_1$ queries this oracle, $\mathcal{C}$ generates the system parameters, and $\mathcal{C}$ randomly selects P and q as the generator and order of group G. Subsequently, $\mathcal{C}$ randomly selects a secret value sk as the TA's key and computes the public key $PK = sk \cdot P$. At last, $\mathcal{C}$ returns all the parameters except sk to $\mathcal{A}_1$. Meanwhile, $\mathcal{C}$ maintains four lists, L_{h_2}, L_{PK}, L_{σ_1}, and L_{σ_2}, which are initially empty.

- ExtractPublicKey(VID): When $\mathcal{A}_1$ calls this query, $\mathcal{C}$ first queries whether the list L_{PK} contains corresponding (X, C_2); if it does contain them, then $\mathcal{C}$ sends (X, C_2) to $\mathcal{A}_1$. Otherwise, $\mathcal{C}$ randomly selects $\sigma_2, x \in Z_q^*$ and $C_1 \in Z_q^*$ and sets $R = \sigma_2 \cdot P - PK \cdot C_1$, $X = x \cdot P$ and $C_2 = H_2(R \parallel X \parallel PK \parallel T_1)$. $\mathcal{C}$ adds (VID_i, X, R, C_2) and $(VID_i, \sigma_2, x, X, R, C_1, C_2)$ to L_{h_2} and L_{PK} separately. Then, $\mathcal{C}$ returns (X, C_2) to $\mathcal{A}_1$.
- $H_1(R, PK)$: When $\mathcal{A}_1$ queries this oracle, $\mathcal{C}$ first looks up its list L_{h_1}. If the entry exist, $\mathcal{C}$ sends C_1 to $\mathcal{A}_1$; otherwise, $\mathcal{C}$ calls ExtractPublicKey(VID) and sends C_1 to $\mathcal{A}_1$.
- $H_2(R, X, PK, T_1)$: When $\mathcal{A}_1$ queries this oracle, $\mathcal{C}$ first looks up its list L_{h_2}. If the entry exist, $\mathcal{C}$ sends C_2 to $\mathcal{A}_1$; otherwise $\mathcal{C}$ calls ExtractPublicKey(VID) (inserts (VID_i, X, R, C_2) into L_{h_2} in this query) and sends C_2 to $\mathcal{A}_1$.
- ExtractSecretValue(VID): In this query, $\mathcal{C}$ searches L_{PK} to find VID_i and the corresponding secret value x. If VID_i does not exist, $\mathcal{C}$ searches L_{PK} after executing the ExtractPublicKey(VID) query and returns an appropriate x to $\mathcal{A}_1$.
- ExtractPartialPrivateKey(VID): When $\mathcal{C}$ receives ExtractPartialPrivateKey(VID) from $\mathcal{A}_1$ for VID_i, $\mathcal{C}$ first checks whether $VID_i = VID_{gt}$ holds, and if it holds, $\mathcal{C}$ aborts. Otherwise, $\mathcal{C}$ queries list L_{PK} and finds σ_2. If the query does not include it, $\mathcal{C}$ calls ExtractPublicKey(VID) and returns σ_2 to $\mathcal{A}_1$.
- ReplacePublicKey(VID, x, X, C_2): When $\mathcal{A}_1$ calls this query, $\mathcal{C}$ searches L_{PK} with VID_i to find the corresponding (VID_i, x, X, C_2). If this query exists in L_{PK}, $\mathcal{C}$ will replace the user's original X, C_2, and x with X', C_2' and x'. If (VID_i, x, X, C_2) is not in L_{PK}, then $\mathcal{C}$ outputs an unknown value $\perp$. The *type-I* attacker $\mathcal{A}_1$ can invoke this query to replace the (X, C_2) of the challenged vehicle.
- ExtractProof(VID): When receiving this query from $\mathcal{A}_1$ regarding VID_i, $\mathcal{C}$ determines whether $VID_i = VID_{gt}$ holds, and if it holds, the challenger $\mathcal{C}$ maintains a list L_σ containing $(VID_i, \sigma_3, C_1, C_2, X)$. If the queried VID_i is not previously created, $\mathcal{C}$ obtains $(\sigma_2, C_1, C_2, x, X)$ from the list L_{PK}. Then, $\mathcal{C}$ calculates $\sigma_3 = \sigma_2 + xC_2$ and adds $(\sigma_3, C_1, C_2, X, VID_i)$ to L_σ. Finally, $\mathcal{C}$ returns (σ_3, C_1, C_2, X) to $\mathcal{A}_1$.
- ForgeProof(): In this query, we assume that $\mathcal{A}_1$ successfully establishes legitimate authentication parameters (σ_3, C_1, C_2, X) such that the following equation holds

$$R = \sigma_3 \cdot P - PK \cdot C_1 - X \cdot C_2 \tag{3}$$

According to the above equation, we derive it as follows:

$$sk \cdot C_1 \cdot P = \sigma_3 \cdot P - x \cdot P \cdot C_2 - r \cdot P \tag{4}$$

Further, by selecting a different C_1 and repeating the above process, we have

$$sk \cdot C_1^{'} \cdot P = \sigma_3^{'} \cdot P - x \cdot P \cdot C_2 - r \cdot P \tag{5}$$

Using the above equation, we derive the following derivation:

$$sk \cdot C_1 \cdot P - sk \cdot C_1^{'} \cdot P = \sigma_3 \cdot P - x \cdot P \cdot C_2 - r \cdot P - \sigma_3^{'} \cdot P - x \cdot P \cdot C_2 - r \cdot P \tag{6}$$

$$(C_1 - C_1^{'}) \cdot sk \cdot P = (\sigma_3 - \sigma_3^{'}) \cdot P \tag{7}$$

According to the above equation, we can calculate $sk = (\sigma_3 - \sigma_3^{'})(C_1 - C_1^{'})^{-1}$. However, this contradicts the ECDLP assumption. Therefore, assuming that the ECDLP is difficult, we propose that the scheme is insurmountable against an *type-I* adversary in the ROM.

Security Definition 2: As the ECDLP in elliptic curves is complex, we propose scheme that is essentially unforgeable against an *type-II* adversary in the ROM.

Type-II Attacker Capabilities: *Type-II* attacker $\mathcal{A}_2$ is identical to $\mathcal{A}_1$; the difference between the $\mathcal{A}_1$ and $\mathcal{A}_2$ attackers is that $\mathcal{A}_2$ is not able to query ReplacePublicKey, and ExtractSign is never queried.

Proof: The formal proof process is similar to that for *Security Definition* 1.

5.3. Simulation Based on ProVerif Tool

We chose ProVerif (PV) to verify the security of the proposed scheme. Proverif is an automatic simulation and verification tool for cryptographic protocols, which can be used to analyze the security properties of various cryptographic protocols, such as asymmetric encryption, hash function, etc. We defined eight events in the PV:

- TARegVu (bitstring): th TA registers the vehicle.
- VuAcTA (bool): The vehicle checks the information sent by the TA.
- RsuAcVu (bool): The RSU successfully authenticates the vehicle in the initial authentication phase.
- RSUReacVu (bool): The RSU successfully authenticates the vehicle in the re-authentication phase.
- VuAcRSU (bool): The vehicle successfully authenticates the RSU.
- TAEnd ( ): The TA completes the proposed protocol.
- VuEnd ( ): The vehicle completes the proposed protocol.
- RSUEnd ( ): The RSU completes the proposed protocol.

We used the PV to verify that the parameters $\{VID, \sigma_2, sk\}$ can be stolen by the adversary and that the defined events are all executed in order. Figure 6 shows the final verification result of the proposed scheme. The PV verification results demonstrate that our scheme ensures that adversaries are incapable of obtaining the parameters $\{VID, \sigma_2, sk\}$, and all events are executed in order.

```
Verification summary:

Query not attacker(VID[]) is true.
Query not attacker(skTA) is true.
Query not attacker(s2[]) is true.
Query inj-event(TAEn(beacon)) ==> inj-event(VuReg(beacon)) is true.
Query inj-event(TAReg(beacon)) ==> inj-event(TAEn(beacon)) is true.
Query inj-event(VuVerif(cheak)) ==> inj-event(TAReg(beacon)) is true.
Query inj-event(VuAuth(beacon)) ==> inj-event(VuVerif(cheak)) is true.
Query event(RsuVerif(cheak)) ==> event(VuAuth(beacon)) is true.
```

Figure 6. The verification result of the code.

5.4. Informal Security Analysis

The analysis revealed the following:

- MITM Attack: According to the model defined in this article, the user transmits the message over an insecure channel, so the adversary can intercept the message of the user's transmission. In the registration phase and the initial authentication phase, the adversary can intercept $\{P_{vid}, C_{vid}, R, \sigma_1, \sigma_2, X\}$, etc. We protect the VID utilizing the ECDHP. Similarly, the adversary fails to acquire r and$x$ from R and X because of the ECDL problem. In this way, the private keys of the TA and vehicle, utilized for authentication, remain hidden from adversaries. In the re-authentication phase, due to the ECDDH and ECCDH difficulty problems of the elliptic curve, the adversary cannot obtain the parameters used by the vehicle user for authentication next time after intercepting the N, M, and E parameters.
- Anonymity and Unlinkability: According to the above analysis, the adversary cannot obtain the VID and private key used in the authentication through the insecure channel. Furthermore, the private key used for subsequent authentication is generated by the RSU after the last authentication is completed, and the message sent by each authentication is different. Consequently, the anonymity and unlinkability of the vehicle are guaranteed in the NBP.

- Traceability and Revocability: In the BPA, parameter R assumes a crucial role in the authentication process. This parameter corresponds to the genuine identity of the vehicle and is recorded by the TA. And the TA can track a vehicle based on this parameter. Meanwhile, the RSU can upload the vehicle revocation transaction to the blockchain, indicating that the vehicle has been revoked. Therefore, the BPA satisfies the traceability and revocable requirements.
- Replay Attack: In the BPA, the initial authentication phase and re-authentication phase both use timestamps T_1, T_2, and T_3 to indicate the information sending time, respectively. When the RSU and vehicle receive a message from each other, they first verify the validity of the timestamp. In addition, in the timestamp of C_2, M and σ_3 are protected by $H()$, elliptic curve mathematical difficulties, and the XOR operation, so that the adversary cannot replace the timestamp. Once the adversary replaces the timestamp, the message cannot be verified.
- Impersonation Attack: In the BPA, it is impossible for an illegal vehicle to impersonate a legitimate vehicle for authentication. In the registration phase, the vehicle uses the public key PK of the TA and encrypts VID using ElGamal encryption with an elliptic curve, and only the TA can decrypt it using the private key sk. When the TA sends the σ_1 to the vehicle, the private key σ_2 of the vehicle is encrypted using VID. Since the vehicle VID is known only to the vehicle and TA, the adversary cannot obtain the σ_2. In the authentication phase, the vehicle uses random numbers to encrypt the private key σ_2. In the re-authentication phase, the RSU and the vehicle share the next authentication private key of the vehicle with their own private key and secret number, respectively. Therefore, the adversary cannot create a valid authentication message $\{\sigma_3, C_1, C_2, X, T_1\}$ or $\{\sigma_4, N, T_3\}$ by intercepting the message sent by the vehicle. The BPA can prohibit simulated attacks.
- Session Fixation Attack: A session fixation attack is the use of fixed parameters present in messages sent by communicating parties to hijack other sessions or simulate other objects [5]. In the BPA, all parameters in each authentication message are different, and there are no fixed parameters, so adversaries cannot hijack other sessions or simulate other objects, and the BPA is resistant to session fixation attacks.
- Forward Secrecy: In the BPA, it is assumed that the adversary obtains the current session key, but the random numbers n and m are only used once in the current session, and they updated after each identity authentication to ensure that each secret is fresh in the current session, so the adversary cannot obtain the previous information, ensuring forward security.
- Colluding Attack Resistance: In the proposed scheme, a collusion attack refers to multiple illegal/compromised vehicles colluding together to obtain the TA key sk. The TA sends the key $\sigma_1 = r + skC_1 + C_1VID$ to the vehicle in the registration phase, and the vehicle can decrypt $\sigma_2 = r + skC_1$ through its own VID. However, there is an unknown number r in this parameter, and the vehicle cannot obtain r through R due to the ECDHP. At the same time, the r of each vehicle is different, so sk and r are unknown to the adversary, and the sk cannot be obtained. Our scheme is resistant to colluding attacks.

6. Performance Analysis

This section provides a comprehensive comparison of our scheme with other schemes in terms of security features and computing and communication costs. When it comes to a computational cost evaluation, we selected a supersingular elliptic curve $E : y^2 = x^3 + ax + b \ mod \ q$ on a finite field F_q, where $a, b \in Z_q$ and p, q. We ran the simulation experiment on a personal computer (Intel Core i5-10500@3.10GHz CPU, 8.00 GB of random memory with a Windows 10 operating system, and the manufacturer is HP).

6.1. Security Feature Comparison

As shown in Table 2, we compared the security features of the BPA with those of existing authentication schemes, where "√" means that the scheme satisfies the corresponding security features, and " × " means that the feature is not satisfied.

The results presented in Table 2 show that our scheme has robust security features. B-TSCA [32], SEA [37], and BPAS [38] fail to provide unlinkability; a malicious attacker may infer the real identity of the vehicle based on its authentication information, thus revealing the privacy of the vehicle. In addition, Amar's scheme [28] and SEA [37] fail to provide traceability and revocation and may prevent tracing the identity of malicious vehicles, resulting in malicious message propagation, which poses a threat to the security of the IoV.

Table 2. Security feature comparison.

Authentication	Anonymity	Unlinkability	Traceability	Revocable
ZAMA [29]	√	√	√	√
B-TSCA [32]	√	×	√	√
Amar's scheme [28]	√	√	×	×
SEA [37]	√	×	×	×
BPAS [38]	√	×	√	√
BPA	√	√	√	√

6.2. Computational Costs

The running times of different operations is shown in Table 3. We considered that the time required for XOR operations is very short and can be ignored. We conducted an analysis of the registration, authentication, and re-authentication processes for BPA, ZAMA [29], and B-TSCA [32], calculating the time costs associated with each phase of these schemes, which are summarized in Table 4 and Figure 7. ZAMA [29] uses ZKP based on FO Commitment and elliptic curve cryptography for authentication, mainly uses modular exponentiation operations, modular addition operations, modular multiplication operations, etc. B-TSCA [32] mainly uses bilinear pairing operations, modular exponentiation operations, modular multiplication operations, etc. And the BPA mainly uses elliptic curve point multiplication operations, elliptic curve point addition operations, modular addition operations, modular multiplication operations, etc. As shown in Table 4, our scheme spends less time in the authentication and re-authentication phases than ZAMA [29] and B-TSCA [32]. Although our scheme spends more time in the registration phase, this phase is generally executed only once before the authentication phase for a vehicle. However, the re-authentication phase needs to be performed multiple times, so our scheme has more advantages.

Table 3. Execution time of basic operations (ms).

Abbreviations	Operations	Time (ms)
T_{mul}^{ecc}	Elliptic curve point multiplication operation	0.2330
T_{add}^{ecc}	Elliptic curve point addition operation	0.2330
T_{sub}^{ecc}	Elliptic curve point subtraction operation	0.0162
T_{mul}^{mod}	Modular multiplication operation	0.0031
T_{add}^{mod}	Modular addition operation	0.2330
T_{div}^{mod}	Modular division operation	0.0169
T_{exp}^{mod}	Modular exponentiation operation	0.0931
T_h	SHA-256 hash operation	0.0055
T_{enc}^{ecc}	Ellipse curve encryption operation	1.0741
T_{dec}^{ecc}	Ellipse curve decryption operation	0.4780
T_{bp}	Bilinear pairing operation	4.7559

Table 4. Comparison of computational costs.

Scheme	Registration Phase Cost	Authentication Phase Cost	Re-Authentication Phase Cost
ZAZM [29]	$11T_{exp}^{mod} + T_{mul}^{mod} \approx 1.0295$ ms	$11T_{exp}^{mod} + 5T_{mul}^{mod} + 4T_{add}^{mod} + T_{div}^{mod} + T_h + T_{enc}^{ecc} + T_{dec}^{ecc} \approx 2.6435$ ms	$2T_{exp}^{mod} + T_{mul}^{mod} + T_{div}^{mod} + T_{enc}^{ecc} + T_{dec}^{ecc} \approx 1.7606$ ms
B-TSCA [32]	-	$6T_{exp}^{mod} + 3T_{mul}^{mod} + 4T_h + 2T_{bp} \approx 10.1086$ ms	$6T_{exp}^{mod} + 4T_{mul}^{mod} + 2T_h + 2T_{bp} \approx 10.1030$ ms
BPA	$7T_{mul}^{ecc} + 3T_{add}^{ecc} + T2_{add}^{mod} + T_{sub}^{ecc} + 2T_h \approx 1.6764$ ms	$8T_{mul}^{ecc} + 2T_{sub}^{ecc} + T_{add}^{mod} + 3T_h + T_{mul}^{mod} \approx 1.9106$ ms	$7T_{mul}^{ecc} + 2T_{add}^{mod} + 3T_{add}^{ecc} + T_h \approx 1.6547$ ms

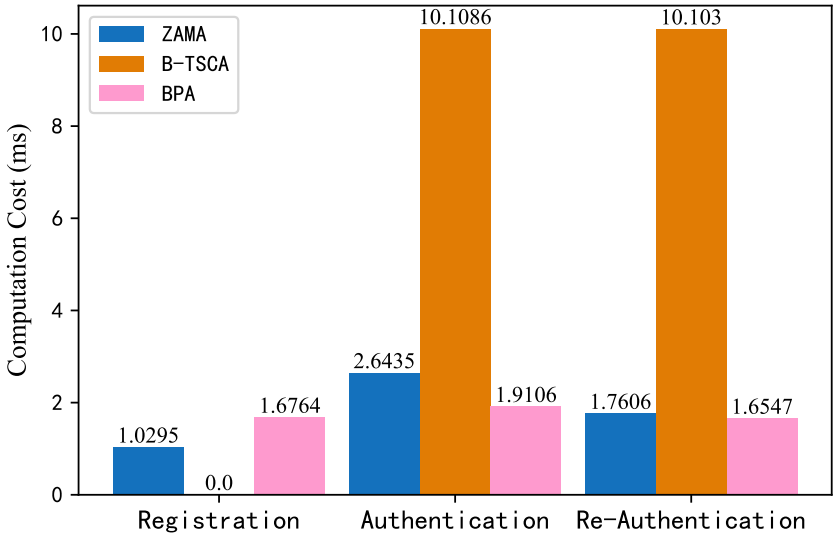

Figure 7. Comparison of computational costs.

6.3. Communication Costs

The sizes of the parameters used in the authentication process are a very important factor in the communication costs. So, we referred to several metrics, including the sizes of the points in group G (64 bytes), random numbers in Z_q^* (32 bytes), the vehicle VIDs (8 bytes), and the timestamps (8 bytes). Table 5 and Figure 8 shows the communication overhead of ZAMA [29], B-TSCA [32], and BPA in different phases. Through the comparison in Figure 8, it is evident that our scheme has a lower overhead in every stage compared to ZAMA [29]. This is because ZAMA [29] requires elliptic curve encryption for each message, which increases the communication overhead. Compared with B-TSCA [32], the BPA has a higher communication cost, but B-TSCA [32] needs to query the trust value of related vehicles before authentication, which also demands a certain communication overhead. Moreover, our scheme has a lower computational overhead at each stage than B-TSCA [32]. Additionally, the B-TSCA [32] scheme fails to provide unconnectability and has a slight lack of security. In contrast, our scheme has more advantages.

Table 5. Comparison of communication costs (bytes).

Scheme	Registration Phase Cost	Authentication Phase Cost	Re-Authentication Phase Cost
ZAZM [29]	456	1200	472
B-TSCA [32]	-	72	136
BPA	232	386	240

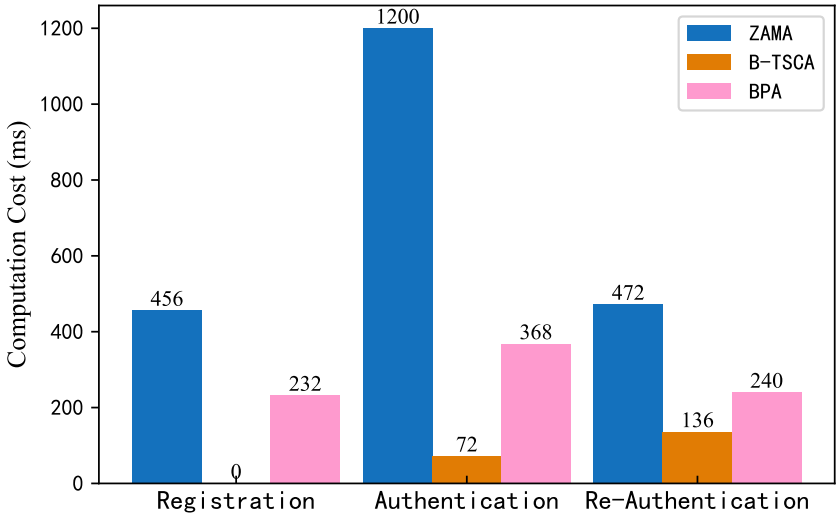

Figure 8. Comparison of communication costs.

7. Open Challenges and Future Research Directions

The scheme proposed in this paper ensures the secure and efficient authentication of vehicles in the IoV. However, the introduction of blockchain technology, which is known to have bottlenecks in terms of storage and consensus, poses challenges. Specifically, when the number of vehicle authentication requests in the IoV is high, the volume of data that blockchain needs to process and store increases sharply, exerting pressure on the storage capacity of the nodes. Therefore, future research is expected to explore an optimized blockchain storage model aimed at alleviating the storage burden on nodes while maintaining the system's efficient operation and data security. Additionally, there is a desire to investigate a more efficient blockchain consensus protocol to enhance the speed of data sharing among RSUs.

8. Conclusions

This paper proposes an efficient authentication scheme assisted by blockchain technology. In this scheme, vehicles authenticate with an RSU, while the TA is mainly responsible for vehicle registration and tracing. This strategic distribution addresses the communication and computing bottlenecks associated with centralized authentication schemes. An RSU can re-authenticate vehicles through the blockchain to reduce computational overhead. Based on a security evaluation, the BPA can ensure vehicle anonymity, providing unlinkability and traceability, and is more secure than the traditional anonymous authentication scheme. Compared with other schemes, our scheme incurs lower costs in the authentication and re-authentication phases. In future work, we will further improve the efficiency of the scheme and apply it to practical IoV systems.

Author Contributions: Conceptualization, J.L. and Y.L. (Yuanyuan Lin); methodology, Y.L. (Yuanyuan Lin); validation, J.L., Y.L. (Yibing Li), Y.Z. and Y.C.; formal analysis, Y.L. (Yuanyuan Lin); investigation, Y.L. (Yuanyuan Lin); data curation, Y.L. (Yuanyuan Lin); writing—original draft preparation, Y.L. (Yuanyuan Lin); writing—review and editing, J.L., Y.L. (Yibing Li), Y.Z. and Y.C.; visualization, Y.L. (Yuanyuan Lin). All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China under Grant 62302458.

Data Availability Statement: Data are contained within the article.

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

References

1. Dong, Z.; Jing, C.; Guo, R.; Gao, S.; Wang, L. A Traceable Blockchain-Based Access Authentication System with Privacy Preservation in VANETs. *IEEE Access* **2019**, *7*, 117716–117726.
2. Liu, X.; Huang, H.; Xiao, F.; Ma, Z. A Blockchain-Based Trust Management with Conditional Privacy-Preserving Announcement Scheme for VANETs. *IEEE Internet Things J.* **2020**, *7*, 4101–4112. [CrossRef]
3. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet Things J.* **2018**, 5, 3701–3709. [CrossRef]
4. Aman, M.; Javaid, U.; Sikdar, B. A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles. *IEEE Internet Things J.* **2020**, 8, 1123–1139. [CrossRef]
5. Xu, Z.; Liang, W.; Li, K.; Xu, J.B.; Jin, H. A Blockchain-Based Roadside Unit-Assisted Authentication and Key Agreement Protocol for Internet of Vehicles. *J. Parallel Distrib. Comput.* **2021**, 149, 29–39. [CrossRef]
6. Li, J.T.; Li, Y.F.; Cao, C.H.; Lam, K.-Y. Conditional Anonymous Authentication with Abuse-Resistant Tracing and Distributed Trust for Internet of Vehicles. *IEEE Internet Things J.* **2022**, 9, 8749–8762. [CrossRef]
7. Lin, C.; Huang, X.Y.; He, D.B. EBCPA: Efficient Blockchain-Based Conditional Privacy-Preserving Authentication for VANETs. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20*, 1818–1832. [CrossRef]
8. Wang, S.B.; Yao, N.M. LIAP: A Local Identity-Based Anonymous Message Authentication Protocol in VANETs. *Comput. Commun.* **2017**, *112*, 154–164. [CrossRef]
9. Zhou, X.T.; He, D.B.; Khan, M.K.; Wu, W.; Choo, K.R. An Efficient Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for VANETs. *IEEE Trans. Veh. Technol.* **2023**, *72*, 81–92. [CrossRef]
10. Fei, W.; Xu, Y.J.; Zhang, H.W.; Zhang, Y.J.; Zhu, L.H. 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET. *IEEE Trans. Veh. Technol.* **2015**, *65*, 896–911.
11. Li, J.L.; Ji, Y.S.; Kim-Kwang, R.C.; Dieter, H. CL-CPPA: Certificate-Less Conditional Privacy-Preserving Authentication Protocol for the Internet of Vehicles. *IEEE Internet Things J.* **2019**, *6*, 10332–10343. [CrossRef]
12. Wang, P.; Chen, C.M.; Saru, K.; Mohammad, S.; Rahim, T. HDMA: Hybrid D2D Message Authentication Scheme for 5G-Enabled VANETs. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5071–5080. [CrossRef]
13. Huang, H.P.; Zhu, P.; Xiao, F.; Sun, X.; Huang, Q.L. A Blockchain-Based Scheme for Privacy-Preserving and Secure Sharing of Medical Data. *Comput. Secur.* **2020**, *99*, 102010. [CrossRef] [PubMed]
14. Gao, S.; Peng, Z.; Tan, F.; Zheng, Y.Q.; Xiao, B. SymmeProof: Compact Zero-knowledge Argument for Blockchain Confidential Transactions. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 2289–2301. [CrossRef]
15. Raya, M.; Hubaux, J. Securing Vehicular Ad Hoc Networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [CrossRef]
16. Qiu, H.; Qiu, M.; Lu, R. Secure V2X Communication Network based on Intelligent PKI and Edge Computing. *IEEE Netw.* **2019**, *34*, 172–178. [CrossRef]
17. Heng, X.; Qin, S.; Xiao, Y.; Wang, J.; Tao, Y.; Zhang, R. A Strong Secure V2I Authentication Scheme from PKI and Accumulator. In Proceedings of the 2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 14–16 January 2022; pp. 98–103.
18. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
19. Ma, M.; He, D.; Wang, H.; Kumar, N.; Choo, K.K.R. An Efficient and Provably Secure Authenticated key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks. *IEEE Internet Things J.* **2019**, *6*, 8065–8075. [CrossRef]
20. Awais, S.M.; Yucheng, W.; Mahmood, K.; Kharel, R. Comments on "An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks". In Proceedings of the 2023 IEEE 6th International Conference on Electronics and Communication Engineering (ICECE), Xi'an, China, 15–17 December 2023; pp. 229–233.
21. Tabany, M.; Syed, M. A Lightweight Mutual Authentication Protocol for Internet of Vehicles. *J. Adv. Inf. Technol.* **2024**, *15*, 155–163. [CrossRef]
22. Chen, Y.; Chen, J. CPP-CLAS: Efficient and Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme for VANETs. *IEEE Internet Things J.* **2021**, *9*, 10354–10365. [CrossRef]
23. Xu, Z.; Wang, L.; Luo, Y.; Long, Y.; Zhang, K.; Yan, H.; Chen, K. A Security-Enhanced Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme for Vehicular Ad-Hoc Networks. *IEEE Internet Things J.* **2023**, *11*, 13482–13495. [CrossRef]
24. Kamil, I.A.; Ogundoyin, S.O. An Improved Certificateless Aggregate Signature Scheme without Bilinear Pairings for Vehicular Ad Hoc Networks. *J. Inf. Secur. Appl.* **2019**, *44*, 184–200. [CrossRef]
25. Zhao, Y.; Hou, Y.; Wang, L.; Kumari, S.; Khan, M.K.; Xiong, H. An Efficient Certificateless Aggregate Signature Scheme for the Internet of Vehicles. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3708. [CrossRef]
26. Han, Y.; Song, W.; Zhou, Z.; Wang, H.; Yuan, B. eCLAS: An Efficient Pairing-Free Certificateless Aggregate Signature for Secure VANET Communication. *IEEE Syst. J.* **2021**, *16*, 1637–1648. [CrossRef]
27. Zheng, H.; Luo, M.; Zhang, Y.; Peng, C.; Feng, Q. A Security-Enhanced Pairing-Free Certificateless Aggregate Signature for Vehicular Ad-Hoc Networks. *IEEE Syst. J.* **2022**, *17*, 3822–3833. [CrossRef]
28. Amar, A.R.; Rabi, N.M.; Felix, G.H. Adaptive Group-Based Zero Knowledge Proof-Authentication Protocol in Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 867–881.

29. Xi, N.; Li, W.; Jing, L.; Ma, J. ZAMA: A ZKP-Based Anonymous Mutual Authentication Scheme for the IoV. *IEEE Internet Things J.* **2022**, *9*, 22903–22913. [CrossRef]
30. Varma, I.M.; Kumar, N. ZKP-Based Lightweight Authentication Protocol during Handovers in Vehicular Networks. In Proceedings of the GLOBECOM 2023—2023 IEEE Global Communications Conference, Kuala Lumpur, Malaysia, 4–8 December 2023; pp. 868–873.
31. Meng, X.; Xu, J.; Liang, W.; Xu, Z.; Li, K. A Lightweight Anonymous Cross-Regional Mutual Authentication Scheme using Blockchain Technology for Internet of Vehicles. *Comput. Electr. Eng.* **2021**, *95*, 107431. [CrossRef]
32. Wang, C.; Shen, J.; Lai, J.; Liu, J. B-TSCA: Blockchain Assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1386–1396. [CrossRef]
33. Xie, Q.; Ding, Z.; Tang, W.; Tan, X. Provable Secure and Lightweight Blockchain-Based V2I Handover Authentication and V2V Broadcast Protocol for VANETs. *IEEE Trans. Veh. Technol.* **2023**, *12*, 72. [CrossRef]
34. Tao, Q.; Ding, H.; Jiang, T.; Cui, X. B-DSPA: A Blockchain-Based Dynamically Scalable Privacy-Preserving Authentication Scheme in Vehicular Ad-hoc Networks. *IEEE Internet Things J.* **2023**, *11*, 1385–1397. [CrossRef]
35. Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese Remainder Theorem based Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-hoc Networks. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 722–735. [CrossRef]
36. Wang, W.; Xu, H.; Alazab, M.; Gadekallu, T.; Han, Z.; Su, C. Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7059–7067. [CrossRef]
37. Shen, M.; Lu, H.; Wang, F.; Liu, H.; Zhu, L. Secure and Efficient Blockchain-Assisted Authentication for Edge-Integrated Internet-of-Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 12250–12263. [CrossRef]
38. Feng, Q.; He, D.; Zeadally, S.; Liang, K. BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4146–4155 [CrossRef]