# Conditional Privacy-Preserving Multi-Domain Authentication and Pseudonym Management for 6G-Enabled IoV

Guanjie Cheng, Junqin Huang, Yewei Wang, Jun Zhao, *Member, IEEE*, Linghe Kong, *Senior Member, IEEE*, Shuiguang Deng, *Senior Member, IEEE*, Xueqiang Yan

***Abstract*—With the emergence of the sixth-generation (6G) communication technologies, the Internet of Vehicles (IoV) is rapidly developing with the coordination between intelligent networked vehicles, road infrastructures, and the cloud. However, the openness and dynamic nature of the IoV raise significant security and privacy concerns, highlighting the need for efficient authentication schemes. Conventional authentication schemes are no longer suitable for 6G-enabled IoV due to high latency, single point of failure, and heavy management costs. Additionally, existing literature on multi-domain authentication mainly investigates vehicle mobility, ignoring the challenges posed by vehicle heterogeneity. To fill this gap, we propose a multi-domain authentication scheme with conditional privacy preservation (MACPP) that considers administrative domains ($AD$) and geographic domains ($GD$) in the IoV. In MACPP, we design a novel identity-based signature scheme without requiring bilinear pairing for efficient authentication. Additionally, we propose a blockchain-assisted pseudonym management scheme (BAPM) to further improve system security by designing a dynamical sparse Merkle tree structure (DSMT). We demonstrate that the proposed MACPP satisfies the security requirements through an in-depth security analysis. Moreover, the experimental results demonstrate the effectiveness and efficiency of both MACPP and BAPM.**

***Index Terms*—Internet of Vehicles, authentication, conditional privacy preservation, identity-based signature, pseudonym management, Merkle tree.**

## I. Introduction

As the critical component of the intelligent transportation systems (ITS), the Internet of Vehicles (IoV) connects the vehicles, roadside units (RSUs), and other networked infrastructures to form a dynamic, heterogeneous, and real-time collaborative network through wireless communication technologies, e.g., the dedicated short-range communication (DSRC) and cellular vehicle-to-everything (C-V2X) [1]. Zeadally *et al.* [2] show that C-V2X performs better than DSRC in communication latency, transmission distance, and reliability. Although 5G-enabled C-V2X has obtained significant developments, it cannot provide intelligent connected management and advanced networking [3]. Besides, there is a trade-off between reliability and latency in the current 5G systems, which causes several challenging issues [4]. Thus, the upcoming exponential increase of the vehicles and the data traffic in the IoV would put 5G under great pressure. Luckily, the deployment of 6G aims to offer ultra-low latency, high availability, strong reliability, and native intelligence capabilities, through involving emerging technologies such as edge intelligence, blockchain, digital twin, quantum communication, and so on [5]. Therefore, 6G is anticipated to bring greater intelligence, safety, and efficiency to V2X applications, making 6G-enabled IoV one of the most noteworthy areas [6].

The IoV improves traffic efficiency and road safety by providing environmental perception, information interaction, and collaborative control capabilities for vehicle driving and traffic management applications. Despite the promising potential of 6G-enabled IoV, it faces several challenges that impede its overall success. The openness and dynamic nature of the IoV make it quite vulnerable to security and privacy threats. Adversaries may launch various attacks to disrupt the normal operation of the system or reveal private information about vehicles, such as the impersonation attack, the modification attack, the message linking attack, and so on. For instance, it is a startling fact that for nearly half a decade, millions of General Motors (GM) cars and trucks were susceptible to a remote exploit. This vulnerability allowed potential adversaries to track vehicles, engage their brakes at high speeds, or even completely disable the braking system, exposing the vehicles and their occupants to significant risks [7]. Therefore, it is important to perform identity authentication before establishing V2X communications. However, conventional centralized authentication approaches present high transmission latency, single point of failure, and heavy management overheads, making them no longer suitable for 6G-enabled IoV [8].

There are two primary issues we should tackle when designing a multi-domain authentication scheme for the IoV system: vehicle mobility and vehicle heterogeneity. Vehicles in motion can traverse multiple geographic domains ($GDs$) at high speeds. Throughout their journey, these vehicles may exchange data with RSUs deployed across different $GDs$

This work was supported in part by the National Key Research and Development Program of China under Grant 2022YFB4500100; in part by the National Science Foundation of China under Grants 62125206 and U20A20173; in part by the Key Research Project of Zhejiang Province under Grant 2022C01145; and in part by Open Research Projects of Zhejiang Lab 2022NL0AB01. *(Corresponding authors: Shuiguang Deng; Jun Zhao.)*

Guanjie Cheng and Shuiguang Deng are with the School of Computer Science and Technology, Zhejiang University, Hangzhou 310007, China, and also with the Hainan Institute of Zhejiang University, Sanya 572025, China (e-mail: n2208144d@e.ntu.edu.sg; dengsg@zju.edu.cn).

Junqin Huang, Yewei Wang, and Linghe Kong are with Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: junqin.huang@sjtu.edu.cn; jakiewangxy@gmail.com; linghe.kong@sjtu.edu.cn).

Jun Zhao is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798 (e-mail: junzhao@ntu.edu.sg).

Xueqiang Yan is with the Wireless Technology Lab of Huawei Technologies Co.,Ltd., Shanghai 201206, China (e-mail: yanxueqiang1@huawei.com).

via V2X communication, which presents potential security risks. For example, a malicious vehicle could relay false driving information to a nearby RSU. Thus, it is vital that moving vehicles and RSUs from various $GDs$ execute mutual authentication to establish secure communication. Moreover, the low-latency and reliable demands of the vehicles require cross-$GD$ authentication services to be both real-time and dependable. Given these challenges, most existing studies concentrate on designing secure and efficient cross-$GD$ authentication schemes [9]–[12]. Nowadays, many vehicle manufacturers attempt to build Certificate Authorities ($CAs$) or Key Generation Centers ($KGCs$) by themselves, aiming to design personalized security mechanisms for enterprise-level IoV systems [13]. Treating a manufacturer as an administrative domain ($AD$), vehicles manufactured by different $ADs$ may obey different authentication schemes and configurations, leading to vehicle heterogeneity. Each $AD$ forms a closed security zone, severely hampering interoperability between vehicles belonging to different $ADs$ [8], [14]. Therefore, it is necessary to design a multi-domain authentication scheme for the IoV, which considers $ADs$ and $GDs$ simultaneously.

Numerous vehicular authentication schemes have been proposed to ensure security in the IoV. These mechanisms can be classified into three categories based on the cryptography used. Most existing schemes rely on the centralized Public Key Infrastructure (PKI) and require certificates issued by a trusted CA to verify vehicle identities. To address the cross-domain authentication problem, Brecht *et al.* [15] designed a CA trust list for all vehicles, but Yang *et al.* [13] found this scheme to be inflexible and costly. Some authentication schemes utilize symmetric cryptography to reduce computational complexity and provide privacy protection [16]. However, these schemes are not suitable for the IoV due to the vulnerability of the symmetric key and the absence of non-repudiation. Other works adopt identity-based cryptography (IBC) to release the pressure of certificate or key management [17]. However, most IBC-based authentication schemes are implemented through bilinear pairing, which requires high computation costs [10]. Moreover, IBC faces the key escrow problem [18]. Although these works aim to achieve secure authentication, they only focus on a single domain type, either $GD$ or $AD$, and lack a holistic investigation of vehicle mobility and heterogeneity.

Another essential requirement in IoV authentication is conditional privacy protection, which ensures the anonymity of vehicles while reserving the right to reveal the real identities of malicious vehicles. For example, survey data indicates that most vehicles are parked approximately 95% of the day on average. This reality, coupled with the analysis of transmitted traffic data such as destinations, parking locations, and intervals, can allow attackers to effectively infer personal activities associated with a targeted vehicle [19]. This situation can pose serious threats to property security and even the personal safety of drivers. However, complete anonymity could potentially enable the dissemination of harmful messages. Malicious vehicles could report fake traffic information like vehicle speed, driving direction, or traffic lights, which could mislead other vehicles and result in traffic congestion or accidents. Thus, it is crucial to design an authentication scheme with conditional privacy preservation. Achieving anonymity by using vehicle pseudonyms is a widely-used solution for conditional privacy preservation [20]. However, many pseudonyms need to be preloaded into the vehicles to avoid the linkability incurred by a single pseudonym, causing a big storage burden. Besides, the current centralized pseudonym management scheme introduces heavy costs and many security issues. Therefore, it is necessary to design an adaptive pseudonym generation scheme and a reliable pseudonym management scheme. In this paper, we propose a multi-domain authentication scheme with conditional privacy preservation (MACPP) for 6G-enabled IoV. Specifically, we design a bilinear pairing-free identity-based signature (IBS) scheme based on Ellipitic Curve Cryptography (ECC) and propose an adaptive pseudonym generation scheme for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) authentication. Additionally, we design a blockchain-assisted pseudonym management scheme (BAPM) through a dynamical sparse Merkle tree structure (DSMT). The security basis for MACPP is provided by two hard problems: Elliptic Curve Discrete Logarithm Problem (ECDLP) and Computational Diffie–Hellman Problem (CDHP) [21].

We summarize the main contributions as follows.

- First, we consider both $ADs$ and $GDs$ in 6G-enabled IoV and propose a multi-domain authentication scheme with conditional privacy preservation (MACPP) through a bilinear pairing-free IBS scheme. To improve performance further, we introduce a batch verification function in MACPP.
- Second, we propose an adaptive pseudonym generation scheme to achieve conditional privacy preservation. Moreover, we design a dynamical sparse Merkle tree structure (DSMT) and propose a blockchain-assisted pseudonym management scheme (BAPM). To the best of our knowledge, this is the first attempt to use Merkle tree alongside blockchain for pseudonym management.
- Third, we conduct an in-depth security analysis to demonstrate that the proposed MACPP can meet the security requirements of 6G-enabled IoV. Moreover, we use the widely recognized Automated Validation of Internet Security Protocols and Applications (AVISPA) software validation tool to perform formal security verification on the proposed authentication scheme.
- Finally, we analyze the computation cost and the communication cost of MACPP. We also evaluate the performance of the proposed BAPM and the blockchain network. The numerical results demonstrate the effectiveness and efficiency of the proposed schemes.

The rest of this paper is organized as follows. The related work is discussed in Section II. We introduce the problem statement, system model, design goals, and some background knowledge in Section III. The proposed MACPP scheme and BAPM scheme are detailed in Section IV and Section V, respectively. Section VI provides formal proof and a detailed analysis of the achieved security properties. Section VII discusses experimental results. Finally, we conclude this work in Section VIII.

## II. Related Work

Blockchain has been envisioned as one of the promising technologies for building trusted 6G-enabled IoVs due to its prominent features, such as decentralization, immutability, consistency, and security [22]. Therefore, many research results have combined blockchain technology to solve identity authentication issues in the IoV. Besides, several privacy-preserving vehicular authentication schemes have been proposed to protect the sensitive information of vehicles in recent years. This section discusses the related works from the perspectives of blockchain-based cross-domain authentication and privacy-protecting authentication.

### A. Blockchain-based Cross-domain Authentication Schemes

As an immutable distributed ledger, blockchain can help establish trust relationships between different domains through consensus algorithms. Yang *et al.* [23] designed a blockchain-enabled scheme to solve the cross-domain authentication problem of heterogeneous terminal devices accessing network services in different communication domains in IoT. However, the device identities are exposed to the public, incurring privacy leakage issues. Dong *et al.* [9] proposed a cross-domain authentication scheme based on inter-blockchain communication. When a mobile device moves from one network to another, the two blockchains communicate to complete the authentication. However, this framework heavily relies on the security of the Cosmos hub, which is vulnerable to single point attacks. Hao *et al.* [11] designed a lightweight consortium blockchain-based architecture to enable cross-domain access control for IoT devices. However, the system cannot provide stable services for devices when more than 1/3 of the full nodes are compromised. Thus, it is unsuitable for the IoV, where service availability needs to be guaranteed. Feng *et al.* [10] deployed private blockchain and consortium blockchain to achieve cross-domain authentication for 5G-enabled Internet of drones. The private blockchain is used for local device management, while the consortium blockchain enables cross-domain information sharing. However, a compromised domain administrator could threaten data security on the consortium blockchain. Yang *et al.* [13] proposed a multi-domain vehicular authentication architecture by introducing blockchain to share cross-domain information among multiple domains. Similarly, Lv *et al.* [12] utilized blockchain to share the public information of devices among edge nodes of different domains. Tong *et al.* [8] presented a blockchain-based complete cross-domain authentication scheme without changing the original authentication scheme within the domain.

While existing literature has proposed various cross-domain authentication schemes, these studies typically focus on a single type of domain, either $GDs$ or $ADs$, lacking a comprehensive examination of both vehicle mobility and heterogeneity. Moreover, some of these schemes do not ensure conditional privacy protection. Thus, multi-domain authentication with conditional privacy-preservation in 6G-enabled IoV remains unsolved but imperative.

### B. Privacy Preserving-oriented Authentication Schemes

Conditional privacy protection is the basic requirement in IoV authentication. Message authentication code (MAC) is widely utilized to perform authentication and verify message integrity [16], [24]. The receiver authenticates the message with a pre-shared key with the sender, with no need to expose the actual identities. However, the large size of the MAC output makes it unsuitable for resource-constrained terminal devices. Furthermore, it lacks non-repudiation. To solve these issues, some works proposed pseudonym certificate-based authentication and pseudonym-changing strategies for vehicle privacy. Ullah *et al.* [25] proposed an Adaptive Grouping and Pseudonym-Changing (AGPC) scheme to shield the factual location information of vehicle users. Haider *et al.* [26] designed a pseudonym generation scheme using Gao Algorithm to reduce memory costs and maximize location confidentiality. However, these methods incur considerable certificate management overheads. Thus, significant research efforts have focused on designing IBS-based authentication schemes with privacy preservation [20], [27]–[31]. However, most of these schemes are based on bilinear pairing, which incurs expensive computation costs. To eliminate the computation costs brought by bilinear pairing, some works proposed pairing-free batch verification-based authentication mechanisms for the IoV [13], [32], [33]. However, these works either ignored pseudonym management or incurred significant management costs. Additionally, while there have been several blockchain-based conditional privacy-preserving authentication schemes proposed recently, Lin *et al.* [7] found that most of these schemes involve high communication overheads and fail to meet the low latency requirements of the IoV.

In summary, the challenge of providing multi-domain authentication with conditional privacy-preservation, along with efficient pseudonym management for 6G-enabled IoV, remains significant and unresolved. To address these gaps in the current literature, we simultaneously consider $ADs$ and $GDs$, designing a lightweight IBS scheme that does not require bilinear pairing. Based on this, we propose a multi-domain authentication scheme that offers conditional privacy preservation. In addition, our scheme supports batch verification for improved efficiency. To further enhance security, we propose a blockchain-assisted pseudonym management scheme.

## III. System Model and Design Goals

In this section, we first summarize the problem statement. Following this, we introduce the system model, security model, and design goals. Lastly, we present some basic knowledge necessary for the proposed scheme.

### A. Problem Statement

The significant security and privacy challenges present in 6G-enabled IoV necessitate the development of a conditional privacy-preserving authentication scheme that simultaneously addresses $ADs$ and $GDs$. Furthermore, existing pseudonym schemes impose substantial costs and fail to meet the low latency requirements of the IoV. As such, our primary goal

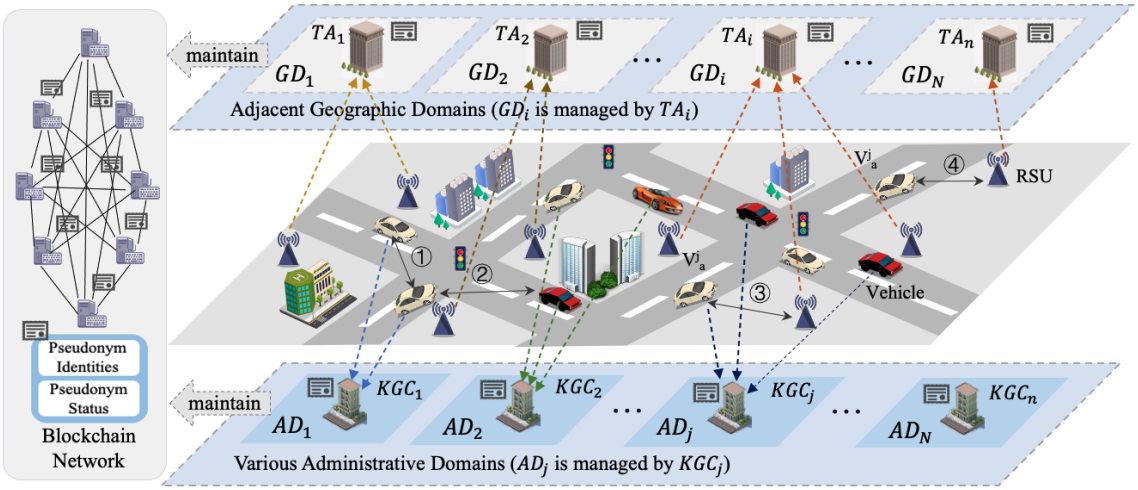



Fig. 1. The system overview for the blockchain-assisted multi-domain IoV. ① indicates intra-AD V2V communication. ② indicates cross-AD V2V communication. ③ and ④ indicate cross-$GD$ V2I communication incurred by the mobility of $V_a^j$. This paper aims to propose a general multi-domain authentication scheme with privacy preservation that can be applied to these three communication scenarios at the same time.

is to establish multi-domain authentication that provides conditional privacy preservation along with efficient and reliable pseudonym management. The specific design goals will be discussed in the following sections.

### B. System Overview and Security Model

The system of a multi-domain IoV is shown in Figure 1. The middle layer represents the practical road traffic, consisting of high-speed moving vehicles, RSUs, and other networked transport equipment that can collect, process, and communicate data. 6G-driven C-V2X is the assumed communication protocol, as it is better suited for advanced IoV applications. The upper layer presents adjacent $GDs$, between which high-speed moving vehicles constantly shuttle. $GD_i$ indicates the $i$-th district and $TA_i$ indicates the corresponding transport authority located in $GD_i$. $TA_i$ defines the traffic policies and technical principles in its district and is responsible for the deployment and management of RSUs. But all $TAs$ follow the unified traffic policy issued by a superior department (denoted as $SD$). Thus, $TAs$ are reliable entities, and they trust each other. The bottom layer presents various vehicle manufacturers, which represent $ADs$ in the IoV. Each $AD$ is managed by its $KGC$, i.e., the independent $CA$ constructed by the manufacturer. $KGC_j$ provides registration services and generates cryptographic materials for vehicles manufactured in $AD_j$. $TAs$ and $KGCs$ cooperate to maintain a consortium blockchain network, where data are stored immutably. Specifically, the blockchain ledger stores pseudonym identities and pseudonym status of vehicles, forming the basis for a transparent and reliable pseudonym management scheme.

The security model is described as follows.

- $TAs$ and $KGCs$ are fully trusted. They always provide reliable services. $TAs$ store the real identities of vehicles locally and keep them confidential. When a vehicle is detected as malicious, $KGCs$ can reveal its identity.
- $RSUs$ are honest-but-curious. $RSUs$ can honestly follow the protocols to broadcast messages, authenticate vehicles, and upload information. However, $RSUs$ are curious about the privacy of vehicles. They may attempt to analyze the received messages and reveal the real identities of vehicles.
- Vehicles can be malicious. For example, 1) an illegal vehicle may forge a valid signature to inject fake messages into the network. 2) A malicious vehicle may attemp to trace the messages in the transmissions and link one message to a specific vehicle [34].
- Additionally, the IoV system is susceptible to several types of attacks, including impersonation, modification, replay, man-in-the-middle (MiTM), and denial of service (DoS) attacks.

### C. Design Goals

We consider the following design goals in this paper.

- *Message Authentication:* The vehicles and RSUs should be able to check the validity of the received messages and verify the authenticity of the message source.
- *Unlinkability:* RSUs and malicious vehicles are not able to link two messages to the same vehicle, i.e., they cannot trace real identities and reveal private information through analyzing messages.
- *Unforgeability:* The attackers cannot forge valid signatures that can be successfully verified by message receivers.
- *Conditional Privacy Preservation:* The real identities of vehicles should be confidential to any other vehicles and RSUs. However, $TAs$ and $KGCs$ have the ability to trace the vehicle's real identity when necessary.
- *Non-repudiation:* Message senders can not deny the sent messages. Thus, if a vehicle is detected that it performed malicious behaviors, it cannot repudiate the charge.

- *Resistance to Attacks:* The proposed authentication scheme should be capable of defending against common attacks, including impersonation, modification, replay, MiTM, and DoS attacks.

Since the broadcast messages in the IoV have to meet the low-latency demand, the designed scheme should have low computation and communication overheads in addition to the above security goals.

### D. Preliminaries

*1) C-V2X:* C-V2X provides two complementary communication modes for the IoV [35]. One is the pass-through mode, in which data transmission is performed between terminals through a side-link interface, known as the PC5 interface, without going through the base station. PC5 refers to a reference point where the User Equipment (UE), i.e., mobile handset, directly communicates with another UE over the direct channel. PC5 can achieve V2V, V2I, Vehicle-to-Pedestrian (V2P), and other pass-through communications. The other is the cellular mode called Uu, which follows traditional cellular communication and uses the uplink and downlink between the terminal and the base station to implement Vehicle-to-Network (V2N) communications. In this paper, we focus on the V2X communication over PC5.

*2) ECDLP and CDHP:* The proposed scheme is enabled by two hard problems: ECDLP and CDHP. Specifically, given an additive group $G$ consisting of the points on an elliptic curve and the point at infinity, let $P$ denotes the generator and $q$ represents the order. Let $a \in Z_q^*$, and $aP \in G$. The ECDLP states that it is hard to compute $a$ with knowledge of $aP$. Let $b \in Z_q^*$ and $bP \in G$. The CDHP states that it is hard to compute $abP$ with knowledge of $aP$ and $bP$. These two difficult problems provide the security basis for the designed authentication scheme.

*3) Merkle Tree:* Merkel tree is a kind of binary hash tree where every leaf is labeled with the cryptographic hash of a data block, and every node that is not a leaf is labeled with the cryptographic hash of the labels of its child nodes. An example of a Merkle tree is shown in Figure 2. Merkle tree is a fundamental component of blockchain technology since it provides efficient data storage and membership verification [36]. We can use Merkle proofs to validate the existence of the data in the Merkle tree. As shown in Figure 2, if we want to prove data "A" is included in the latest block, the Merkle proof composed of $H(B)$ and $H(H(C) \parallel H(D))$ is required. With "A", $H(B)$, and $H(H(C) \parallel H(D))$, we can recompute the root hash. If the computed root hash equals the Merkle Root recorded in the current block, we can conclude that "A" exists.

## IV. Proposed MACPP scheme

In this section, we introduce the proposed MACPP. We divide the scheme procedures into four phases: the system initialization phase, the enrollment and pseudonym generation phase, the message signing phase, and the verification phase. Furthermore, as an extension to MACPP, we present a batch verification function, allowing multiple signatures to be verified simultaneously. Note that MACPP is a general authentication solution that can be applied to the three V2X communication scenarios presented in Figure 1. The notations used are detailed in Table I. The overview of the proposed scheme is illustrated in Figure 3. We describe the detailed procedures of each phase as follows.

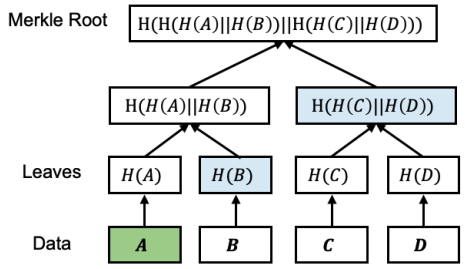



Fig. 2. An example of a Merkle tree.

TABLE I
Notation Description.

| Notation | Description |
|---|---|
| $p, q$ | two large prime numbers |
| $E$ | an elliptic curve |
| $G$ | an additive group with the order $q$ |
| $P$ | a generator of the group $G$ |
| $V_a^j$ | the vehicle $a$ in $AD_j$ |
| $VID_a^j, PID_a^j$ | the real identity and pseudonym of $V_a^j$ |
| $(TP_{pk_i}, tp_i)$ | the key pairs of $TA_i$ |
| $Tag_j$ | the unique label assigned by $KGC_j$ |
| $H(\cdot), h_1, h_2, h_3$ | one time hash algorithm |
| $AEnc(PK, M)$ | asymmetric encryption function using $PK$ to encrypt $M$ |
| $\Omega$ | a table maintained by each $TA$ |
| $\oplus$ | the exclusive-OR operation |
| $\parallel$ | the message concatenation operation |
| / | no value |

### A. System Initialization

In practical IoV systems, the $SD$ is equipped with sufficient computation and communication resources, which is responsible for generating system parameters, managing all $TAs$ and $KGCs$, and making real-time decisions based on the uplink transport messages. The $SD$ chooses an additive group $G$ with order $q$, which is composed of the points on an elliptic curve $E$: $y^2 = x^3 + ax + b \ (mod\ p)$ and the point at infinity $O$, where $a, b \in F_p$ and $p, q$ are two large prime numbers. We denote $P$ as the generator of $G$. The $SD$ defines three secure hash functions $h_1$, $h_2$, $h_3$, where $h_1 : G \rightarrow Z_q^*$, $h_2 : \{0,1\}^* \rightarrow Z_q^*$, $h_3 : G \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^*$. Then, the public parameters $Params = \{G, P, p, q, a, b, h_1, h_2, h_3\}$ are broadcast in the network.

$TA_i$ ($i \in Z_q^*$) chooses a random number $tp_i \in Z_q^*$ as the system private key and computes the system public key as $TP_{pk_i} = tp_i \cdot P$. Afterward, $TA_i$ transmits $TP_{pk_i}$ to each RSU in its region via the wired channel. The RSUs broadcast $TP_{pk_i}$ to all vehicles periodically in the network.

### B. Enrollment and Pseudonym Generation

The vehicle manufacturer distributes a unique identity to each vehicle, containing the vehicle type, production time, and other manufacturing parameters. Before hitting the road, each vehicle must register real identity information with $TA$. Therefore, each $TA$ maintains a table of real identities of all vehicles, denoted as $\Omega$, which achieves its consistency among all $TAs$ through an offline synchronization mechanism enabled by $SD$. We assume the authentic identity of vehicle $a$ in $AD_j$ (denoted as $V_a^j$) is $VID_a^j$. Then the manufacturer will share the identity information of vehicles with its $KGC$ to generate cryptographic materials for secure authentication. $KGC_j$ randomly selects a secret number $Tag_j \in Z_q^*$ as a unified label proving that the vehicles with $Tag_j$ belong to $AD_j$. $KGC_j$ computes $TAG_j = Tag_j \cdot P$ and broadcasts it in the network. $KGC_j$ pre-loads $\{VID_a^j, AD_j, Tag_j\}$ into the on-board unit (OBU) of the vehicles before they come into operation. Note that the OBU is a tamper-proof device and the information stored in it can never be disclosed or falsified [20]. Therefore, $Tag_j$ is always safe and confidential even if the vehicles are scrapped or attacked.

Supposing $V_a^j$ wants to generate a pseudonym identity, it triggers a request to its OBU through security mechanisms such as password verification or fingerprint recognition, which is pre-designed by the vehicle manufacturer and is out of the scope of this paper. The OBU generates a random number $\kappa_a^j \in Z_q^*$ and computes $PID_{a,1}^j = \kappa_a^j \cdot P$, $PID_{a,2}^j = VID_a^j \oplus h_1(\kappa_a^j \cdot TAG_j) \oplus AD_j$. Hence, $PID_a^j = \{PID_{a,1}^j, PID_{a,2}^j\}$ is defined as the pseudonym of $V_a^j$. Afterward, the OBU calculates $\alpha_a^j = h_2(PID_a^j \parallel T_a^j)$ and $sk_a^j = \kappa_a^j + \alpha_a^j \cdot Tag_j \ mod \ q$, where $T_a^j$ is the current timestamp. $\alpha_a^j$ and $sk_a^j$ are signature materials of $V_a^j$ for V2X authentication. Finally, the OBU sends $\{PID_a^j, sk_a^j, T_a^j\}$ to $V_a^j$.

### C. Message Signing

We assume $V_a^j$ intends to broadcast a traffic-warning message $M_a^j$ to nearby vehicles and RSUs, which may include information regarding traffic conditions such as road defects, congestion status, and more. Based on these messages, other vehicles can take timely actions to adjust driving behavior to improve road safety and traffic efficiency. $V_a^j$ generates a random number $w_a^j \in Z_q^*$ and computes $W_a^j = w_a^j \cdot P$, $\beta_a^j = h_3(W_a^j \parallel M_a^j \parallel AD_j \parallel PID_a^j \parallel T_a^j)$, and $\sigma_a^j = sk_a^j + \beta_a^j \cdot w_a^j \ mod \ q$. As a result, $\{W_a^j, \sigma_a^j\}$ is the signature of $\{M_a^j, AD_j, PID_a^j, T_a^j\}$. Finally, $V_a^j$ broadcasts $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^j, T_a^j\}$ to nearby vehicles and RSUs.

### D. Verification

Malicious attackers may intentionally broadcast fake messages to mislead the vehicles, harming the IoV system. Thus, the vehicles and RSUs need to check the validity and integrity of the received messages timely before taking further actions. First, the verifier checks the freshness of $T_a^j$ and rejects the message if it is not fresh. Then, the verifier checks whether $PID_a^j$ is valid, which will be discussed in Section V. Finally, the verifier calculates $\alpha_a^j$ and $\beta_a^j$ using the parameters in the received message and the system parameters $Params$. It checks whether the equation $\sigma_a^j \cdot P = PID_{a,1}^j + \alpha_a^j \cdot TAG_j + \beta_a^j \cdot W_a^j$ holds. If the equation does not hold, the verifier rejects the message; otherwise, the verifier accepts the message.

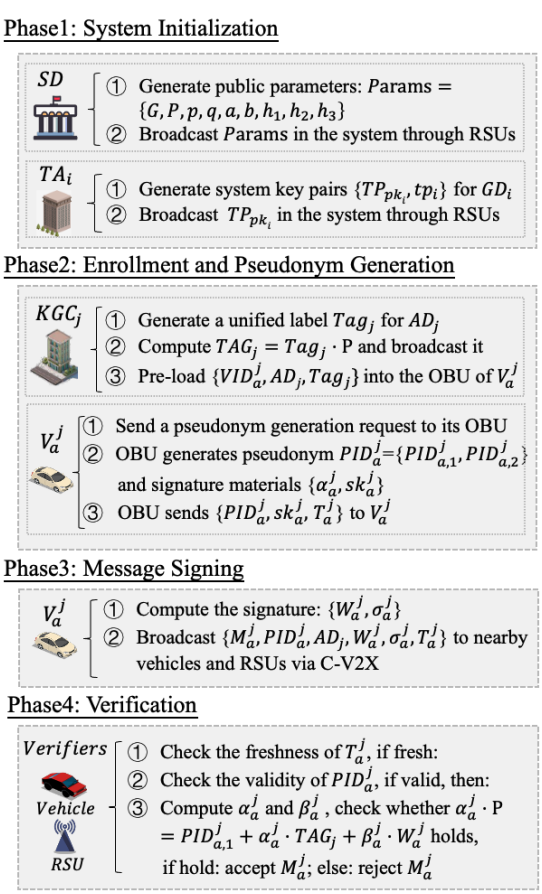



Fig. 3. The overview of MACPP.

*Proof.* If the signature is computed correctly by $V_a^j$, we can rigorously get that

$$\begin{aligned} \sigma_a^j \cdot P &= (sk_a^j + \beta_a^j \cdot w_a^j) \cdot P \\ &= (\kappa_a^j + \alpha_a^j \cdot Tag_j + \beta_a^j \cdot w_a^j) \cdot P \\ &= \kappa_a^j \cdot P + \alpha_a^j \cdot Tag_j \cdot P + \beta_a^j \cdot w_a^j \cdot P \\ &= PID_{a,1}^j + \alpha_a^j \cdot TAG_j + \beta_a^j \cdot W_a^j. \end{aligned} \tag{1}$$

Therefore, the correctness of the signature verification is proved. □

### E. Extension for Batch Verification of Multiple Signatures

As the number of vehicles in 6G-enabled IoV continues to grow, there will be an increase in the frequency of communications and a larger data volume. A vehicle or RSU may receive multiple messages broadcasted by nearby vehicles or RSUs simultaneously. However, due to the overload of processing capacity, incoming events may be discarded, leading to a loss of valuable information [3]. Additionally, validating received messages one by one introduces high latency, which can severely impact a vehicle's real-time decision-making on

driving behavior. To address these issues, we design a batch verification scheme for the proposed signature scheme.

One of the biggest difficulties in designing a batch verification scheme under the multi-domain IoV scenario is that the message senders may come from various $ADs$ (i.e., vehicle manufacturers). We assume a verifier receives messages $\Phi = \{\phi_1, \phi_2, \ldots, \phi_j\}$, which are defined as follows:

$\phi_1$**:** $\phi_1$ is a message set defined by $\{\{M_1^1, PID_1^1, AD_1, W_1^1, \sigma_1^1, T_1^1\}, \{M_2^1, PID_2^1, AD_1, W_2^1, \sigma_2^1, T_2^1\}, \ldots, \{M_n^1, PID_n^1, AD_1, W_n^1, \sigma_n^1, T_n^1\}\}$, which are sent by vehicles $\{V_1^1, V_2^1, \ldots, V_n^1\}$ from $AD_1$, respectively.

$\phi_2$**:** $\phi_2$ is a message set defined by $\{\{M_1^2, PID_1^2, AD_2, W_1^2, \sigma_1^2, T_1^2\}, \{M_2^2, PID_2^2, AD_2, W_2^2, \sigma_2^2, T_2^2\}, \ldots, \{M_m^2, PID_m^2, AD_2, W_m^2, \sigma_m^2, T_m^2\}\}$, which are sent by vehicles $\{V_1^2, V_2^2, \ldots, V_m^2\}$ from $AD_2$, respectively.

$\phi_j$**:** And $\phi_j$ is a message set defined by $\{\{M_1^j, PID_1^j, AD_j, W_1^j, \sigma_1^j, T_1^j\}, \{M_2^j, PID_2^j, AD_j, W_2^j, \sigma_2^j, T_2^j\}, \ldots, \{M_z^j, PID_z^j, AD_j, W_z^j, \sigma_z^j, T_z^j\}\}$, which are sent by vehicles $\{V_1^j, V_2^j, \ldots, V_z^j\}$ from $AD_j$, respectively.

The verifier checks the validity of the above messages through the following steps.

1) The verifier checks the freshness of the timestamp included in each message. If the timestamp is not fresh, the verifier rejects the message. Otherwise:
2) The verifier checks whether the following equation holds. If the equation does not hold, the verifier rejects the messages; otherwise, the verifier accepts the messages.

$$\begin{aligned}\left(\sum_{i=1}^{n}\sigma_i^1 + \sum_{i=1}^{m}\sigma_i^2 + \cdots + \sum_{i=1}^{z}\sigma_i^j\right)\cdot P = \sum_{i=1}^{n} PID_{i,1}^1 \\ + \sum_{i=1}^{m} PID_{i,1}^2 + \cdots + \sum_{i=1}^{z} PID_{i,1}^j + \left(\sum_{i=1}^{n}\alpha_i^1\right)\cdot TAG_1 \\ + \left(\sum_{i=1}^{m}\alpha_i^2\right)\cdot TAG_2 + \cdots + \left(\sum_{i=1}^{z}\alpha_i^j\right)\cdot TAG_j \\ + \sum_{i=1}^{n}(\beta_i^1 \cdot W_i^1) + \sum_{i=1}^{m}(\beta_i^2 \cdot W_i^2) + \cdots + \sum_{i=1}^{z}(\beta_i^j \cdot W_i^j).\end{aligned} \tag{2}$$

*Proof.* For simplicity, we assume the verifier receives $n$ messages and all senders come from $AD_j$. If the signatures are computed correctly, we can rigorously get that

$$\begin{aligned}\left(\sum_{i=1}^{n}\sigma_i^j\right)\cdot P = \sum_{i=1}^{n}(sk_i^j + \beta_i^j \cdot w_i^j)\cdot P = \\ \sum_{i=1}^{n}(\kappa_i^j + \alpha_i^j \cdot Tag_j)\cdot P + \sum_{i=1}^{n}(\beta_i^j \cdot w_i^j \cdot P) = \\ \sum_{i=1}^{n} PID_{i,1}^j + \left(\sum_{i=1}^{n}\alpha_i^j\right)\cdot TAG_j + \sum_{i=1}^{n}(\beta_i^j \cdot W_i^j).\end{aligned} \tag{3}$$

If Equation (3) holds, it indicates that all $n$ signatures are valid. Otherwise, it suggests that some of the messages in the batch are invalid. In this case, binary search technology can be leveraged to identify the invalid messages [37]. □

**Complexity Analysis:** The overheads of simple operations such as addition in $Z_q^*$ and hashing are omitted. If the verifier verifies the received $n$ signatures one by one according to Equation (1), the normal costs are $3n$ point multiplication operations and $2n$ point addition operations. If the verifier uses the batch verification function according to Equation (3), the expected costs are $(n+2)$ point multiplication operations and $(2n+2)$ point addition operations. We find that the extended batch verification scheme is much more efficient due to the significant reduction in point multiplication operations.

## V. Proposed BAPM Scheme

The proposed MACPP enables vehicles to generate pseudonyms by themselves. However, a malicious or revoked vehicle could generate a new pseudonym and broadcast a fake message to nearby intelligent vehicles, leading to serious security risks. Therefore, the pseudonyms need to be censored and managed uniformly by superior authorities like $TAs$. It is also crucial to have a transparent mechanism for message receivers to verify the validity of pseudonyms quickly and reliably. If a pseudonym is invalid, the receiver should reject the message immediately. To tackle these challenges, we propose a distributed pseudonym management scheme based on a novel data structure called DSMT. Leveraging blockchain technology, our DSMT-based scheme achieves transparency, security, and scalability. The proposed scheme consists of five parts: system initialization, pseudonym generation or update, pseudonym verification and upload, pseudonym enrollment and storage, and pseudonym revocation.

### A. System Initialization

The proposed BAPM scheme involves the cooperation of $TAs$ and $KGCs$ to maintain a consortium blockchain network. Each $KGC$ stores the entire blockchain ledger on local servers for real-time detection and transparent supervision. $KGCs$ also participate in consensus execution to synchronize blocks with $TAs$ and ensure data consistency. Note that $KGCs$ are more computationally efficient since they do not need to perform operations related to pseudonym management. We propose a new data structure, DSMT, specifically designed for storing blockchain data, which forms the basis of our efficient pseudonym management scheme. DSMT is a complete binary hash tree where each data block is given a unique index, and the empty leaves are set to $H(null)$. The DSMT structure is dynamic, as its length is determined by the number of pseudonyms packed by $TA$ (denoted as $TA_i$) in the latest block. Futhermore, the sparsity of DSMT allows for large sections of the tree to be cached, due to the presence of constant values in preset nodes such as $H(null)$, $H(H(null) \parallel H(null))$, and others. Figure 4 depicts an example of the DSMT structure, in which $TA_i$ stores pseudonyms sequentially in the latest block according to the enrollment time, and each pseudonym corresponds to a certain index. $TA_i$ records the pseudonym indices of each vehicle into $\Omega$. Note that the pseudonym indices in DSMT are different from the real identity indices of vehicles to prevent attackers from correlating pseudonyms with real vehicles. For example, in Figure 4, the vehicle $V_a^j$ has two valid pseudonyms, i.e., $PID_a^j$ and $PID_a^{j}$'. The dotted boxes in Figure 4 are preset nodes that

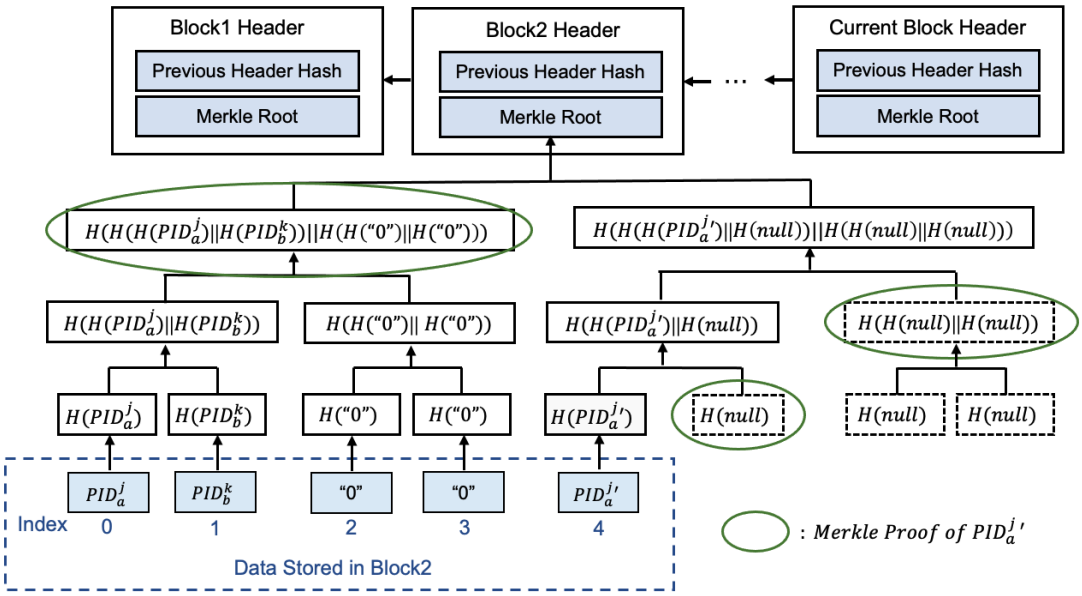



Fig. 4. An example of the proposed DSMT structure.

do not need to be stored. Therefore, DSMT greatly reduces storage overheads. The nodes in Figure 4 circled in green make up the membership proof of $PID_a^j$'.

We present an initialized instance of $\Omega$ in Table II. $\gamma$ and $\delta$ denotes the real-world index of $V_a^j$ and $V_b^k$ respectively, which are irrelevant to pseudonym index. $Idx_1$, $Idx_2$, and $Idx_3$ denote the indices of the leaves in DSMT that store the pseudonyms of $V_b^k$. From Table II, we find that $V_a^j$ has no pseudonym, and $V_b^k$ has three valid pseudonyms.

TABLE II
AN INITIALIZED INSTANCE OF $\Omega$

| Vehicle Index | Real Identity | Pseudonym Index |
|---|---|---|
| $\gamma$ | $VID_a^j$ | / |
| $\delta$ | $VID_b^k$ | $\{Idx_1, Idx_2, Idx_3\}$ |

TABLE III
THE INSTANCE OF $\Omega$ AFTER PSEUDONYM ENROLLMENT OF $V_a^j$ AND PSEUDONYM REVOCATION OF $V_b^k$

| Vehicle Index | Real Identity | Pseudonym Index |
|---|---|---|
| $\gamma$ | $VID_a^j$ | $\{Idx_a\}$ |
| $\delta$ | $VID_b^k$ | Revoked |

### B. Pseudonym Generation or Update

We consider a scenario in which a vehicle $V_a^j$, needs to generate a new pseudonym or update an existing one for the purpose of authentication and communication within the IoV system. First, $V_a^j$ triggers a request to its OBU. Then, the OBU generates a random number $\kappa_a^j \in Z_q^*$ and computes $PID_{a,1}^j = \kappa_a^j \cdot P$, $PID_{a,2}^j = VID_a^j \oplus h_1(\kappa_a^j \cdot TAG_j) \oplus AD_j$. $PID_a^j = \{PID_{a,1}^j, PID_{a,2}^j\}$ is the pseudonym of $V_a^j$.

### C. Pseudonym Verification and Upload

Pseudonyms cannot be used until the enrollment process is completed. Therefore, $V_a^j$ must synchronize with $TA_i$ after generating the new pseudonym. $V_a^j$ computes $AEnc(TP_{pk_i}, VID_a^j)$ and packages a message $M_{en} = \{PID_a^j, AEnc(TP_{pk_i}, VID_a^j), T_{en}\}$, where $T_{en}$ is the current timestamp. Then, $V_a^j$ signs $M_{en}$ using the scheme described in Section IV-C and unicasts $M_{en}$ and the signature to the nearest RSU for verification. The receiver verifies the signature to check the authenticity and integrity of $M_{en}$ using the scheme described in Section IV-D. If the verification is successful, the receiver uploads $M_{en}$ to its linked $TA$ (denoted as $TA_i$) through the wired channel. Otherwise, it rejects the message. Upon receiving the message, $TA_i$ uses $tp_i$ to decrypt $AEnc(TP_{pk_i}, VID_a^j)$ and obtain the real identity of $V_a^j$, i.e., $VID_a^j$. Afterward, $TA_i$ queries the vehicle index of $VID_a^j$ from $\Omega$, represented by $\gamma$.

### D. Pseudonym Enrollment and Storage

$TA_i$ checks whether $VID_a^j$ is a revoked vehicle according to the records in $\Omega$ and terminates the pseudonym enrollment if $V_a^j$ has been revoked. Otherwise, $TA_i$ stores $PID_a^j$ to the first empty node in the current DSMT, indexed by $Idx_a$. Then, $TA_i$ calculates $H(PID_a^j)$ and updates the Merkle Root in the new block. Finally, $TA_i$ links the new block to the blockchain and records $Idx_a$ into $\Omega$, as shown in Table III.

Other vehicles and RSUs can quickly check the validity of the pseudonyms in the received messages through the blockchain network. For example, if a vehicle wants to check the legitimacy of a pseudonym $PID_a^j$, it queries the membership proof of $H(PID_a^j)$ from the latest block in the blockchain. The pseudonym is valid if the vehicle can reconstruct the root $RT'$ using the membership proof such that $RT'$ equals the Merkle Root included in the latest block. Otherwise, the vehicle directly rejects the message.

### E. Pseudonym Revocation

One of the primary responsibilities of $TAs$ is to revoke the pseudonyms of malicious or damaged vehicles to guarantee the reliability and security of the IoV system. The proposed BAPM provides an efficient way for pseudonym revocation. Specifically, if $TA_i$ determines to revoke the pseudonyms of $V_b^k$, it queries the pseudonym index set of $V_b^k$ from $\Omega$. Then, $TA_i$ replaces all pseudonyms with "0" in DSMT according to the pseudonym index set and stores $H(\text{"0"})$ in the leaves of the corresponding indices in the current block. Afterward, $TA_i$ updates the Merkle Root and links the new block to the blockchain. Finally, $TA_i$ eliminates the pseudonym index set of $V_b^k$ and remarks "Revoked" in $\Omega$, as shown in Table III.

## VI. Security Analysis

In this section, we analyze the security of the proposed MACPP scheme. We demonstrate that MACPP can defend against adaptive chosen message attacks based on the ECDLP assumption in the random oracle model. Then, we analyze the required security properties in the design goals described in Section III-C. Furthermore, we conduct formal verification through the widely-used AVISPA tool.

### A. Formal Analysis

We define the security model of MACPP through a game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. $\mathcal{A}$ is able to make the following queries in the game.

- *Setup-Oracle*: $\mathcal{C}$ generates the private key and the system parameters $Params$. Then, $\mathcal{C}$ sends $Params$ to $\mathcal{A}$.
- $h_1$-*Oracle*: Upon receiving $\mathcal{A}$'s query with the message $m_1$, $\mathcal{C}$ chooses a random number $rm_1 \in Z_q$, stores the tuple $(m_1, rm_1)$ into the list $L_{h_1}$, and returns $rm_1$ to $\mathcal{A}$.
- $h_2$-*Oracle*: Upon receiving $\mathcal{A}$'s query with the message $m_2$, $\mathcal{C}$ chooses a random number $rm_2 \in Z_q$, stores the tuple $(m_2, rm_2)$ into the list $L_{h_2}$, and returns $rm_2$ to $\mathcal{A}$.
- $h_3$-*Oracle*: Upon receiving $\mathcal{A}$'s query with the message $m_3$, $\mathcal{C}$ chooses a random number $rm_3 \in Z_q$, stores the tuple $(m_3, rm_3)$ into the list $L_{h_3}$, and returns $rm_3$ to $\mathcal{A}$.
- *Sign-Oracle*: Upon receiving $\mathcal{A}$'s query with the message $M_a^j$, $\mathcal{C}$ generates $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^j, T_a^j\}$ and responses to $\mathcal{A}$.

**Theorem 1.** *MACPP can resist the adaptive chosen message attack under the random oracle model.*

*Proof.* Suppose that an adversary $\mathcal{A}$ can forge a message $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^j, T_a^j\}$. We can construct a challenger $\mathcal{C}$, which can solve ECDLP with a negligible probability by running $\mathcal{A}$ as a subroutine. Given an instance $(P, Q = x \cdot P)$ of ECDLP, $\mathcal{C}$ simulates oracles queried by $\mathcal{A}$ as follows.

- *Setup-Oracle*: $\mathcal{C}$ sets $TAG_j \leftarrow Q$ and sends $Params = \{P, TAG_j, p, q, a, b, h_1, h_2, h_3\}$ to $\mathcal{A}$.
- $h_1$-*Oracle*: $\mathcal{C}$ maintains a list $L_{h_1}$ with the form of $(m_1, \tau)$, which is initialized to be empty. Upon receiving $\mathcal{A}$'s query with the message $m_1$, $\mathcal{C}$ checks if there is a tuple $(m_1, \tau)$ in $L_{h_1}$. If so, $\mathcal{C}$ returns $\tau = h_1(m_1)$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ chooses a random number $\tau \in Z_q$, stores $(m_1, \tau)$ in $L_{h_1}$, and sends $\tau = h_1(m_1)$ to $\mathcal{A}$.
- $h_2$-*Oracle*: $\mathcal{C}$ maintains a list $L_{h_2}$ with the form of $(PID_a^j, T_a^j, \tau)$, which is initialized to be empty. Upon receiving $\mathcal{A}$'s query with the message $\{PID_a^j, T_a^j\}$, $\mathcal{C}$ checks if there is a tuple $(PID_a^j, T_a^j, \tau)$ in $L_{h_2}$. If so, $\mathcal{C}$ returns $\tau = h_2(PID_a^j \parallel T_a^j)$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ chooses a random number $\tau \in Z_q$, stores $(PID_a^j, T_a^j, \tau)$ in $L_{h_2}$, and sends $\tau = h_2(PID_a^j \parallel T_a^j)$ to $\mathcal{A}$.
- $h_3$-*Oracle*: $\mathcal{C}$ maintains a list $L_{h_3}$ with the form of $(W_a^j, M_a^j, AD_j, PID_a^j, T_a^j, \tau)$, which is initialized to be empty. Upon receiving $\mathcal{A}$'s query with the message $\{W_a^j, M_a^j, AD_j, PID_a^j, T_a^j\}$, $\mathcal{C}$ checks if there is a tuple $(W_a^j, M_a^j, AD_j, PID_a^j, T_a^j, \tau)$ in $L_{h_3}$. If so, $\mathcal{C}$ returns $\tau = h_3(W_a^j \parallel M_a^j \parallel AD_j \parallel PID_a^j \parallel T_a^j)$ to $\mathcal{A}$. Otherwise, $\mathcal{C}$ chooses a random number $\tau \in Z_q$, stores $(W_a^j, M_a^j, AD_j, PID_a^j, T_a^j, \tau)$ in $L_{h_3}$, and sends $\tau = h_3(W_a^j \parallel M_a^j \parallel AD_j \parallel PID_a^j \parallel T_a^j)$ to $\mathcal{A}$.
- *Sign-Oracle*: Upon receiving $\mathcal{A}$'s query with the message $M_a^j$, $\mathcal{C}$ selects three random numbers $\sigma_a^j$, $\alpha_a^j$, and $\beta_a^j \in Z_q^*$. $\mathcal{C}$ chooses a random point $PID_{a,2}^j$ and computes $PID_{a,1}^j = \sigma_a^j \cdot P - \alpha_a^j \cdot TAG_j - \beta_a^j \cdot W_a^j$. $\mathcal{C}$ adds $(PID_a^j, T_a^j, \alpha_a^j)$ and $(W_a^j, M_a^j, AD_j, PID_a^j, T_a^j, \beta_a^j)$ into $L_{h_2}$ and $L_{h_3}$ respectively. Finally, $\mathcal{C}$ sends the message $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^j, T_a^j\}$ to $\mathcal{A}$. The signatures generated by $\mathcal{C}$ are indistinguishable from those generated by authenticated vehicles since the equation $\sigma_a^j \cdot P = PID_{a,1}^j + \alpha_a^j \cdot TAG_j + \beta_a^j \cdot W_a^j$ always holds.

Next, $\mathcal{A}$ sends a message $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^j, T_a^j\}$ to $\mathcal{C}$. $\mathcal{C}$ checks if the following equation holds.

$$\sigma_a^j \cdot P = PID_{a,1}^j + \alpha_a^j \cdot TAG_j + \beta_a^j \cdot W_a^j. \tag{4}$$

If not, $\mathcal{C}$ discards the process. According to the forgery lemma [38], $\mathcal{A}$ can output another valid message $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^{j*}, T_a^j\}$, where $\sigma_a^{j*} \neq \sigma_a^j$. Thus, we can get the following equation.

$$\sigma_a^{j*} \cdot P = PID_{a,1}^j + \alpha_a^{j*} \cdot TAG_j + \beta_a^j \cdot W_a^j. \tag{5}$$

From Equations (4) and (5), we can get

$$\begin{aligned}(\sigma_a^j - \sigma_a^{j*}) \cdot P &= \sigma_a^j \cdot P - \sigma_a^{j*} \cdot P \\ &= PID_{a,1}^j + \alpha_a^j \cdot TAG_j + \beta_a^j \cdot W_a^j \\ &\quad - (PID_{a,1}^j + \alpha_a^{j*} \cdot TAG_j + \beta_a^j \cdot W_a^j) \\ &= (\alpha_a^j - \alpha_a^{j*}) \cdot TAG_j \\ &= (\alpha_a^j - \alpha_a^{j*}) \cdot Tag_j \cdot P.\end{aligned} \tag{6}$$

At last, $\mathcal{C}$ outputs $Tag_j = (\alpha_a^j - \alpha_a^{j*})^{-1}(\sigma_a^j - \sigma_a^{j*})$ as a solution to the ECDLP. However, it is contradictory to the hardness of the ECDLP. Therefore, the theorem is proved. □

### B. Informal Analysis

*1) Message Authentication:* Upon receiving a message $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^j, T_a^j\}$, a verifier can first check the legality of $PID_a^j$ via blockchain. Then, it can check the validity and integrity of the message by verifying whether the equation $\sigma_a^j \cdot P = PID_{a,1}^j + \alpha_a^j \cdot TAG_j + \beta_a^j \cdot W_a^j$ holds. Thus, the proposed MACPP scheme provides message authentication.

*2) Unlinkability:* First, the pseudonym $PID_a^j$ is generated secretly based on a random number $\kappa_a^j$ by the OBU. An attacker cannot deduce the real identity of the vehicle from the pseudonym. Second, the vehicles are able to generate multiple pseudonyms. No adversary could link several messages or pseudonyms to the same vehicle. Therefore, unlinkability is achieved in MACPP.

*3) Unforgeability:* The generated signatures can not be forged due to the computational complexity of ECDLP, as proved in Section VI-A. In the batch verification process outlined in Section IV-E, there is a potential threat of adversaries intercepting and misusing previously validated messages to craft deceptive signatures to bypass the batch verification. Specifically, after intercepting $m$ valid messages $\{M_i^j, PID_i^j, AD_j, W_i^j, \sigma_i^j, T_i^j\}$ $(i \in [1,m])$, adversaries might craft false signatures $\{\sigma_i^{j'}\}$ $(i \in [1,m])$ such that $\sum_{i=1}^{m} \sigma_i^{j'} = \sum_{i=1}^{m} \sigma_i^j$ and forward new sets of messages $\{M_i^j, PID_i^j, AD_j, W_i^j, \sigma_i^{j'}, T_i^{j'}\}$ $(i \in [1,m])$ targeting a specific vehicle or RSU. However, this form of attack is avoided by the timestamp requirement of the proposed MACPP. Every newly transmitted message must embed a fresh timestamp that is synchronized with the global clock to prevent against replay attacks. Additionally, every new timestamp $T_i^{j'}$ uniquely dictates values for $\alpha_i^{j'}$ and $\beta_i^{j'}$. However, the confidentiality of $\kappa_i^j$, $Tag_j$, and $w_i^j$ prevents adversaries from accurately deriving the associated $\sigma_i^{j'}$ for a given timestamp $T_i^{j'}$, where $\sigma_i^{j'} = sk_i^{j'} + \beta_i^{j'} \cdot w_i^j \ mod\ q$ and $sk_i^{j'} = \kappa_i^j + \alpha_i^{j'} \cdot Tag_j \ mod\ q$. As a result, the verifier will detect such forgeries during the evaluation of Equation (2). Therefore, the proposed MACPP scheme can achieve unforgeability.

*4) Conditional Privacy Preservation:* In MACPP, dynamically renewable pseudonyms enable privacy preservation of the vehicle's real identity. The pseudonym of $V_a^j$ is composed of $PID_{a,1}^j$ and $PID_{a,2}^j$, where $PID_{a,1}^j = \kappa_a^j \cdot P$, $PID_{a,2}^j = VID_a^j \oplus h_1(\kappa_a^j \cdot TAG_j) \oplus AD_j$. Supposing $V_a^j$ is detected to be a malicious vehicle, $KGC_j$ can extract its real identity by computing $VID_a^j = PID_{a,2}^j \oplus h_1(PID_{a,1}^j \cdot Tag_j) \oplus AD_j$. Note that vehicles and RSUs with the knowledge of $TAG_j$ and $PID_a^j$ are unable to compute $PID_{a,1}^j \cdot Tag_j$ and deduce $VID_a^j$ due to the hardness of CDHP. Thus, MACPP can achieve conditional privacy preservation.

*5) Non-repudiation:* A vehicle cannot deny that it has sent a message due to the unforgeability of the signature. Once a misbehavior is detected, verifiers can link the signature to a specific pseudonym and reveal the real vehicle with the help of $KGCs$. Therefore, MACPP can achieve non-repudiation.

*6) Resistance to Attacks:*

- Impersonation attack: To impersonate a valid vehicle, the attacker must generate a message $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^j, T_a^j\}$, satisfying the equation $\sigma_a^j \cdot P = PID_{a,1}^j + \alpha_a^j \cdot TAG_j + \beta_a^j \cdot W_a^j$. According to Theorem 1, it is impossible to generate this message due to the difficulty of ECDLP. Thus, the proposed MACPP scheme can withstand the impersonation attack.
- Modification attack: Any modification to the message breaks the message integrity and could be checked by verifying whether the equation $\sigma_a^j \cdot P = PID_{a,1}^j + \alpha_a^j \cdot TAG_j + \beta_a^j \cdot W_a^j$ holds. Thus, the proposed MACPP scheme can resist the modification attack.
- Replay attack: We include a timestamp in each message $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^j, T_a^j\}$ to avoid a replay attack. Verifiers can find the replay of the messages by checking the freshness of the timestamp. Therefore, the proposed MACPP scheme can resist the replay attack.
- MiTM attack: Once received, each message will be authenticated through signature verification. Thus, whether the message is from the claimed legal source can be verified. Therefore, the proposed MACPP scheme can withstand the man-in-the-middle attack.
- DoS attack: DoS attacks can be averted by preventing the adversary from gaining unauthorized access [39]. If the signature verification fails, the sender will be considered unauthenticated and access will be denied. This can effectively prevent adversaries from disabling the system through resource consumption. As a result, the proposed MACPP scheme can effectively resist DoS attacks.

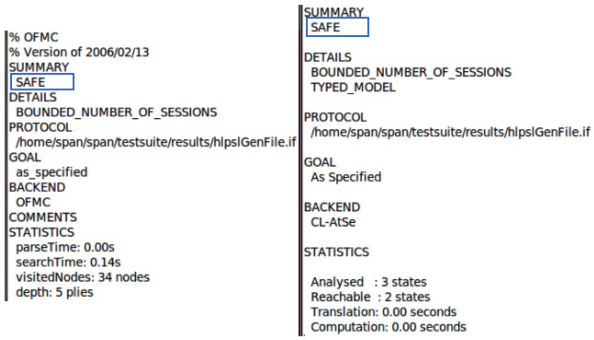



Fig. 5. Simulation results using OFMC & CL-AtSe backends.

### C. Formal Security Verification Using AVISPA

AVISPA is a well-known simulation tool used to evaluate the security of a protocol against both passive and active adversaries, such as replay and MiTM attacks [40]. It features four backends: 1) on the fly model checker (OFMC); 2) constraint logic-based attack searcher (CL-AtSe); 3) SATbased model checker (SATMC); and 4) tree automate based on automatic approximations for the analysis of security protocols (TA4SPs). These backends support most existing automatic analysis techniques. Additionally, the protocols to be tested on AVISPA need to be implemented using the High-Level Protocols Specification Language (HLPSL), which is a role-oriented language that includes basic roles representing each participant and composition roles which describe the environments.

We implement the proposed MACPP using HLPSL for four basic roles of a $KGC$, a vehicle, its OBU, and a message receiver, and for the mandatory composition roles. Then, we simulate the authentication phases using the SPAN, the Security Protocol ANimator for AVISPA. We select OFMC and CL-AtSe backends for simulation. The simulation results, depicted in Figure 5, demonstrate the security of our proposed scheme.

TABLE IV
EXECUTION TIME OF CRYPTOGRAPHIC OPERATIONS

| Cryptographic Operation | Execution Time (ms) |
|---|---|
| $TM_{bp}$ | 4.211 |
| $TM_{pm}^{bp}$ | 1.709 |
| $TM_{pa}^{bp}$ | 0.0071 |
| $TM_{pm}^{ecc}$ | 0.442 |
| $TM_{pa}^{ecc}$ | 0.0018 |
| $TM_{ep}$ | 0.072 |
| $TM_{mtp}$ | 4.406 |
| $TM_{h}$ | 0.0001 |

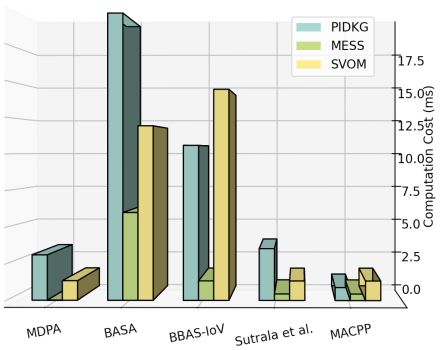



Fig. 6. Computation cost of different phases in MACPP and other schemes.

## VII. Experimental Evaluation

In this section, we evaluate the performance of the proposed schemes through a series of experiments.

### A. Experimental Settings

*1) Environmental Setup:* We build our experimental platform using Node.js v18.13.0 on an Intel(R) Core(TM) i7-10700K 3.8GHz processor with 16GB of memory, running Ubuntu 20.04. The blockchain environment is created using Hyperledger Fabric v2.4.6. The implementation code is publicly available on GitHub at https://github.com/imtypist/MACPP.

*2) Benchmark Schemes:* We adopt four IBS-based privacy-preserving authentication schemes for comparison against MACPP in terms of computation and communication costs.

- **MDPA** [13]. This work proposed a blockchain-based vehicular authentication scheme with conditional privacy protection for multi-domain IoV scenarios.
- **BASA** [30]. This work designed a cross-domain authentication method based on bilinear pairings.
- **BBAS-IoV** [31]. This work designed a blockchain-enabled batch authentication scheme for IoV.
- **Sutrala *et al.*** [32]. This work proposed a conditional privacy-preserving authentication mechanism with batch verification based on pseudo-identity which is generated by cooperating with RSU.

*3) Parameter Settings:* The noble-secp256k1 elliptic curve and SHA-256 hash function are employed in the experiments. The asymmetric cryptographic algorithm used in BAPM is ECIES. The parameter sizes used in the communication cost analysis are defined as follows. The sizes of $AD_j$, $GD_i$, a selected random number, and a timestamp are each set to 4 bytes, and the size of the hash output is 32 bytes. Besides, let the size of the prime $p$ and the order $q$ be 32 bytes. Then the element in group $G$ is 64 bytes.

### B. Experimental Analysis on MACPP

*1) Computation Overheads:* The computation overheads are measured by the time taken to execute the operations in the authentication scheme. The lower, the better. For convenience, we define some notations about execution time as follows. $TM_{bp}$: the execution time of a bilinear pairing operation; $TM_{pm}^{bp}$: the execution time of a point multiplication operation related to bilinear pairing; $TM_{pa}^{bp}$: the execution time of a point addition operation related to bilinear pairing; $TM_{pm}^{ecc}$: the execution time of a point multiplication operation related to ECC; $TM_{pa}^{ecc}$: the execution time of a point addition operation related to ECC. $TM_{ep}$: the execution time of an exponentiation operation. $TM_{mtp}$: the execution time of a hash-to-point operation related to bilinear pairing. $TM_{h}$: the execution time of a general hash operation.

Recent works on authentication have not taken pseudonym management into consideration. For fairness, we analyze the computation and communication overheads of the proposed MACPP scheme, excluding the procedures outlined in Section V-C and V-D. The execution time of the cryptographic operations is computed using MIRACL and the results are listed in Table IV. Let $PIDKG$, $MESS$, $SVOM$, and $BVMM$ denote the phase of pseudo-identity and key generation, message signing, single verification of one message, and batch verification of multiple messages, respectively. The comparative results are shown in Table V. It is worth mentioning that batch verification is not supported in MDPA [13] and BASA [30]. The execution time of different phases in various schemes is presented in Figure 6. Our results indicate that MACPP outperforms other schemes in terms of computation costs in the $PIDKG$ and $SVOM$ phases. Although MDPA is more efficient in $MESS$, it lacks support for batch verification of multiple signatures, which is a critical requirement for practical IoV systems.

Furthermore, we compare the batch verification cost of related schemes as shown in Figure 7. In addition to BASA and Sutrala *et al.*, we also include a recently proposed lightweight batch verification scheme [41] for comparison. The results clearly demonstrate that MACPP performs better as the number of vehicles in a batch increases. For instance, when the vehicle density reaches 200, the computation times are 455.75 ms, 354.36 ms, 177.54 ms, and 90.05 ms, respectively. Thus, MACPP is a more suitable choice for deployment in actual IoV systems. Importantly, it should be noted that the computation complexity of batch verification in MACPP is not impacted by vehicle heterogeneity (i.e., the number of $ADs$) and the distribution of vehicles among different $ADs$.

*2) Communication Overheads:* In this part, we compare the communication overheads with other schemes by calculating the packet sizes transmitted in $PIDKG$, $MESS$, $SVOM$,

TABLE V
COMPARISON OF COMPUTATION COST

| Schemes | $PIDKG$ | $MESS$ | $SVOM$ | $BVMM$ |
|---|---|---|---|---|
| **MDPA** | $7TM_{pm}^{ecc}+1TM_{pa}^{ecc}+6TM_h$ $\approx 3.0964\ ms$ | $TM_h \approx 0.0001\ ms$ | $3TM_{pm}^{ecc}+4TM_{pa}^{ecc}+2TM_h$ $\approx 1.3334\ ms$ | Not supported |
| **BASA** | $3TM_{bp}+4TM_{pm}^{bp}+1TM_{pa}^{bp}$ $+2TM_{ep}+4TM_h$ $\approx 19.6205\ ms$ | $1TM_{bp}+1TM_{pm}^{bp}$ $+1TM_{ep}+1TM_h$ $\approx 5.9921\ ms$ | $2TM_{bp}+2TM_{pm}^{bp}+1TM_{pa}^{bp}$ $+1TM_{ep}+2TM_h$ $\approx 11.9193\ ms$ | Not supported |
| **BBAS-IoV** | $4TM_{pm}^{ecc}+2TM_{mtp}+TM_h$ $\approx 10.5801\ ms$ | $3TM_{pm}^{ecc}+3TM_{pa}^{ecc}$ $+3TM_h$ $\approx 1.3317\ ms$ | $3TM_{bp}+4TM_{pm}^{ecc}+4TM_{pa}^{ecc}$ $+3TM_h \approx 14.4085\ ms$ | $3TM_{bp}+(5n)TM_{pm}^{ecc}+$ $(3n+1)TM_{pa}^{ecc}+(2n+1)TM_h$ $\approx 12.6349+2.2156n\ ms$ |
| **Sutrala *et al.*** | $8TM_{pm}^{ecc}+6TM_h$ $\approx 3.5366\ ms$ | $1TM_{pm}^{ecc}+1TM_h$ $\approx 0.4421\ ms$ | $3TM_{pm}^{ecc}+2TM_{pa}^{ecc}+2TM_h$ $\approx 1.3298\ ms$ | $(4n)TM_{pm}^{ecc}+(2n)TM_{pa}^{ecc}+(2n)T_h$ $\approx 1.7718n\ ms$ |
| **MACPP** | $2TM_{pm}^{ecc}+2TM_h$ $\approx 0.8842\ ms$ | $1TM_{pm}^{ecc}+1TM_h$ $\approx 0.4421\ ms$ | $3TM_{pm}^{ecc}+2TM_{pa}^{ecc}+2TM_h$ $\approx 1.3298\ ms$ | $(n+2)TM_{pm}^{ecc}+(2n+2)TM_{pa}^{ecc}$ $+(2n)TM_h \approx 0.8876+0.4458n\ ms$ |

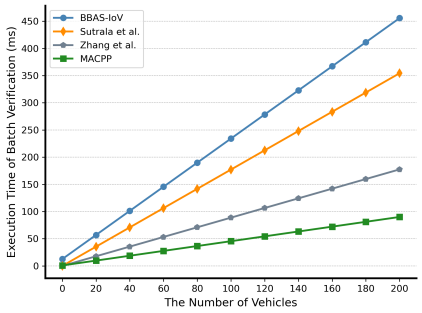



Fig. 7. Execution time for the batch verification of multiple vehicles.

TABLE VI
COMPARISON OF COMMUNICATION COST

| Schemes | $PIDKG$ | $MESS$ | $SVOM$ |
|---|---|---|---|
| **MDPA** | 144 bytes | 236+$S_m$ bytes | 204 bytes |
| **BASA** | 292 bytes | 612+2$S_m$ bytes | 300+$S_m$ bytes |
| **BBAS-IoV** | / | 192+$S_m$ bytes | / |
| **Sutrala *et al.*** | 452 bytes | 360+$S_m$ bytes | / |
| **MACPP** | / | 144+$S_m$ bytes | / |

and $BVMM$, respectively. Let $S_m$ denote the size of the message about traffic status.

There is no network traffic in $PIDKG$ since the pseudonym is locally generated by the vehicle in the proposed MACPP scheme. Besides, the operations in $SVOM$ are also performed locally by the verifier. Thus, the signed messages broadcast by vehicles dominate the communication overheads in MACPP. The vehicle $V_a^j$ broadcasts $\{M_a^j, PID_a^j, AD_j, W_a^j, \sigma_a^j, T_a^j\}$ to other vehicles and RSUs in the vicinity, where $PID_a^j = \{PID_{a,1}^j, PID_{a,2}^j\}$, $PID_{a,1}^j$, $W_a^j \in G$, $PID_{a,2}^j$, $AD_j$, $\sigma_a^j \in Z_q^*$, and $T_a^j$ is a timestamp. Thus, the communication cost of the proposed MACPP scheme is $S_m + 64 \times 2 + 4 \times 4 = 144 + S_m$ bytes. Similarly, we calculate the communication costs of the other schemes by counting the sizes of the packets transmitted in $PIDKG$, $MESS$, and $SVOM$ phases, respectively. The comparative results are shown in Table VI. In BBAS-IoV [31], $S_m$ represents the size of a hello message, which is 332 bytes. MDPA [13] and BASA [30] have communication overheads in all three phases while Sutrala *et al.* [32] has communication costs in $PIDKG$ and $MESS$. It is obvious that the proposed MACPP outperforms the other IBS-based authentication schemes in terms of communication cost.

TABLE VII
EXECUTION TIME OF BAPM

| Procedures | $PG\&U$ | $PV\&U$ | $PE\&S$ | $PR$ |
|---|---|---|---|---|
| Time Cost | 3.595 ms | 5.41 ms | 0.023 ms | 0.023 ms |

### C. Experimental Analysis on BAPM

To evaluate the performance of the proposed DSMT structure, we conduct a comparative analysis with the sparse Merkle tree (SMT) [42] in terms of computation cost and storage cost. Specifically, the proposed DSMT is implemented and compared with SMTs with $2^{16}$, $2^{20}$, and $2^{24}$ leaves. Pseudonym storage and revocation are essentially update operations on the leaves of a Merkle tree. Therefore, we change the number of update operations to observe the computation costs and change the number of pseudonyms to evaluate the storage costs. The results, as illustrated in Figure 8, indicate that the proposed DSMT outperforms SMTs with varying leaf sizes in terms of computation cost. DSMT shows lower execution time due to the fewer hash operations required. Additionally, DSMT has a lower storage cost compared to SMTs, owing to its dynamic height and reduced node storage requirements. For instance, when dealing with 301 pseudonyms, SMTs with $2^{16}$, $2^{20}$, and $2^{24}$ leaves require 19616 bytes, 19744 bytes, and 19872 bytes, respectively, while DSMT requires only 19392 bytes (0.0185 MB). These findings suggest that DSMT is an efficient structure and can be a promising option for pseudonym management in practical IoV applications.

Additionally, we implement Section V-B and V-C to evaluate the efficiency of BAPM. We record the average execution time over 50 experimental runs of each procedure in BAPM. The results are shown in Table VII, where $PG\&U$, $PV\&U$, $PE\&S$, and $PR$ correspond to Section V-B to V-E, respectively. We find that it takes 9.051 ms to perform one complete round of BAPM, demonstrating the efficiency and practicality of the proposed BAPM scheme.

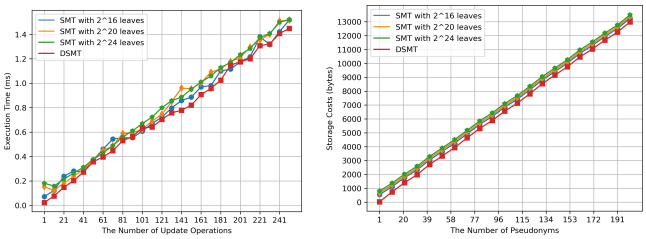



Fig. 8. Comparative analysis of DSMT and SMTs on computation costs (ms) and storage costs (bytes).

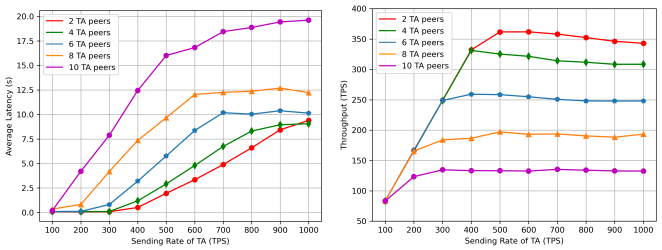



Fig. 9. Average latency and throughput of writing data by $TA$ peers.

### D. Extensive Analysis on Blockchain Network

We introduce blockchain to enable transparent and distributed pseudonym management in the IoV. By storing vehicle pseudonym identities and status through DSMT, we ensure pseudonym synchronization among $TAs$ and $KGCs$, achieving reliable cooperation between $GDs$ and $ADs$ in the IoV. However, the execution of the consensus brings extra latency to the proposed scheme. To evaluate the extra overhead of blockchain synchronization, we deploy writing function using Chaincode in the Fabric platform. $TAs$ and $KGCs$ act as full nodes (i.e., peers) in the network, as shown in Figure 1. $TAs$ record pseudonyms onto the blockchain while the message receivers query the blockchain to verify pseudonym validity.

We focus on two performance metrics: (1) **Extra Latency:** Extra latency is measured by the time taken to reach consensus on new blocks submitted to the blockchain. (2) **Throughput:** Throughput is defined as the number of valid transactions committed per second in the blockchain network. To observe the average latency and transaction throughput under various numbers of $TAs$, we deploy sending rates from 100 to 1000 transactions per second (TPS). As shown in Figure 9, the average latency grows with the sending rate due to the increase in the transaction sort time and verification time. The average delay converges when the verification queue reaches its capacity. Additionally, it indicates that the average latency grows as the number of peer nodes increases. To avoid the impact of the delay caused by pseudonym synchronization on the correctness of the authentication, we can stipulate that a certain period of time is required before a new pseudonym can take effect. The right subfigure in Figure 9 plots the blockchain throughput over different sending rates of writing transactions with various numbers of $TA$ peers. The throughput increases linearly with the sending rate until it converges at a saturation point. Additionally, it shows that more peer nodes yield a lower throughput due to the increased time consumed in consensus. These numerical results can provide guidance for practical blockchain deployments in the IoV.

### E. Practicality Analysis

According to ETSI TS 101 539-2 [43], the maximum end-to-end latency for V2X applications is 300 ms because of the high driving speeds of vehicles. Therefore, in a practical IoV authentication scheme, the sum of the execution time taken in $MESS$ (0.4421 ms for one time according to Table V), the transmission time of the signatures, and the execution time taken in $BVMM$ should be less than 300 ms. Without loss of generality, we assume RSUs are deployed along the roads to manage an area of about 300 meters and the average V2X communication bandwidth is 10 Mbps. We set the size of the traffic-related message (i.e., $S_m$) as 100 bytes, according to [20]. Then the size of the broadcast data packet is $144+100=244$ bytes, according to Table VI. Therefore, the transmission time of a single data packet is $244\ bytes/10\ Mbps\ =\ 0.1952\,ms$.

**Theorem 2.** *The proposed MACPP satisfies the latency requirement in practical IoV systems.*

*Proof.* Let $N_m$ denote the maximum number of signatures aggregated by the message receiver in the batch verification when the latency reaches 300 ms. Then, we have:

$$0.4421 \cdot N_m + 0.1952 \cdot N_m + 0.8876 + 0.4458 \cdot N_m = 300. \quad (7)$$

The calculation result of Equation (7) demonstrates that up to 276 vehicle signatures can be aggregated within the highest acceptable latency. This estimation takes into account the worst-case scenarios, as the signing and transmission phases of various messages can be executed in parallel, leading to a significant reduction in latency. Furthermore, with the advent of 6G technology that promises ultra-high data rates of up to 1 Tbps, the transmission time of one message is expected to be much lower than 0.1952 ms. This implies that the actual number of verified vehicles within an acceptable latency using MACPP is likely to be even higher. Therefore, the proposed scheme meets the requirement in actual IoV systems. □

## VIII. Conclusion

We present a conditional privacy-preserving multi-domain authentication scheme, named MACPP, for 6G-enabled IoV systems that considers the coexistence of $ADs$ and $GDs$. Specifically, we design a novel IBS protocol that does not rely on bilinear pairing, and propose an adaptive pseudonym generation scheme for conditional privacy preservation. The proposed authentication scheme supports batch verification of multiple signatures. Additionally, we introduce a new data structure in blockchain, which forms the basis of our blockchain-assisted pseudonym management scheme. Our security analysis demonstrates that MACPP satisfies the desired security goals while the experimental evaluation shows that it is comparable in terms of computation and communication costs to existing schemes. The numerical results of our evaluation validate the efficacy and efficiency of our proposed

schemes and suggest that MACPP is well-suited for practical IoV systems.

As future work, we intend to quantify the trustworthiness of vehicles in order to evaluate the credibility of received messages and prevent data poisoning attacks.

## REFERENCES


[1] K. Xiong, S. Leng, C. Huang, C. Yuen, and Y. L. Guan, "Intelligent task offloading for heterogeneous v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2226–2238, 2021.

[2] S. Zeadally, M. A. Javed, and E. B. Hamida, "Vehicular communications fo r its: Standardization and challenges," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 11–17, 2020.

[3] W. Li and W. Meng, "Bctrustframe: Enhancing trust management via blockchain and ipfs in 6g era," *IEEE Network*, vol. 36, no. 4, pp. 120–125, 2022.

[4] Y. Hwang and S. Oh, "A study on ultra-reliable and low-latency communication technologies for 5G & 6G services," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 2022, pp. 1207–1209.

[5] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6g internet of things: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 359–383, 2022.

[6] J. Hu, C. Chen, L. Cai, M. R. Khosravi, Q. Pei, and S. Wan, "Uav-assisted vehicular edge computing for the 6g internet of vehicles: Architecture, intelligence, and challenges," *IEEE Communications Standards Magazine*, vol. 5, no. 2, pp. 12–18, 2021.

[7] C. Lin, X. Huang, and D. He, "Ebcpa: Efficient blockchain-based conditional privacy-preserving authentication for vanets," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 1818–1832, 2023.

[8] F. Tong, X. Chen, K. Wang, and Y. Zhang, "Ccap: A complete cross-domain authentication based on blockchain for internet of things," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3789–3800, 2022.

[9] S. Dong, H. Yang, J. Yuan, L. Jiao, A. Yu, and J. Zhang, "Blockchain-based cross-domain authentication strategy for trusted access to mobile devices in the iot," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020, pp. 1610–1612.

[10] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5g-enabled internet of drones," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224–6238, 2022.

[11] X. Hao, W. Ren, Y. Fei, T. Zhu, and K.-K. R. Choo, "A blockchain-based cross-domain and autonomous access control scheme for internet of things," *IEEE Transactions on Services Computing*, pp. 1–1, 2022.

[12] P. Lv, Y. Wang, Y. Wang, C. Liu, Q. Zhou, and Z. Xu, "A highly reliable cross-domain identity authentication protocol based on blockchain in edge computing environment," in *2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2022, pp. 1040–1046.

[13] Y. Yang, L. Wei, J. Wu, C. Long, and B. Li, "A blockchain-based multi-domain authentication scheme for conditional privacy preserving in vehicular ad-hoc network," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8078–8090, 2022.

[14] J. Chen, Z. Zhan, K. He, R. Du, D. Wang, and F. Liu, "Xauth: Efficient privacy-preserving cross-domain authentication," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 3301–3311, 2022.

[15] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.

[16] H. Li, V. Kumar, J.-M. Park, and Y. Yang, "Cumulative message authentication codes for resource-constrained iot networks," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11 847–11 859, 2021.

[17] B. B. Gupta, A. Gaurav, K. T. Chui, and C.-H. Hsu, "Identity-based authentication technique for iot devices," in *2022 IEEE International Conference on Consumer Electronics (ICCE)*, 2022, pp. 1–4.

[18] G. Cheng, Y. Chen, S. Deng, H. Gao, and J. Yin, "A blockchain-based mutual authentication scheme for collaborative edge computing," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 146–158, 2022.

[19] Z. Yang, S. Yu, W. Lou, and C. Liu, "$p^2$ : Privacy-preserving communication and precise reward architecture for v2g networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[20] Y. Yang, L. Zhang, Y. Zhao, K.-K. R. Choo, and Y. Zhang, "Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based vanet," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 317–331, 2022.

[21] F. Sun, S. He, X. Zhang, J. Zhang, Q. Li, and Y. He, "A fully authenticated diffie-hellman protocol and its application in wsns," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1986–1999, 2022.

[22] K. Shah, S. Chadotra, S. Tanwar, R. Gupta, and N. Kumar, "Blockchain for iov in 6g environment: review solutions and challenges," *Cluster Computing*, pp. 1–29, 2022.

[23] L. Yang and J. Liu, "Cross domain authentication based on blockchain for mobile terminals in edge computing environment," in *2021 16th International Conference on Intelligent Systems and Knowledge Engineering (ISKE)*, 2021, pp. 525–529.

[24] P. A. Windya, V. Suryani, and A. A. Wardana, "Sniffing prevention in lora network using combination of advanced encryption standard (aes) and message authentication code (mac)," in *2021 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS)*, 2021, pp. 1–5.

[25] I. Ullah, M. A. Shah, and A. Khan, "Adaptive grouping and pseudonym changing policy for protection of vehicles location information in vanets," in *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2021, pp. 1–7.

[26] S. Haider, D. Gao, R. Ali, A. Hussain, and M. T. Ikram, "A privacy conserves pseudonym acquisition scheme in vehicular communication systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 15 536–15 545, 2022.

[27] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks," *Sensors*, vol. 22, no. 5, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/5/1696

[28] C. Yan, H. Wang, and S. Yan, "An identity-based message authentication scheme for internet of vehicles," in *2022 IEEE 8th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 2022, pp. 154–156.

[29] B. B. Gupta, A. Gaurav, C.-H. Hsu, and B. Jiao, "Identity-based authentication mechanism for secure information sharing in the maritime transport system," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–9, 2021.

[30] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchain-assisted secure device authentication for cross-domain industrial iot," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020.

[31] P. Bagga, A. K. Sutrala, A. K. Das, and P. Vijayakumar, "Blockchain-based batch authentication protocol for internet of vehicles," *Journal of Systems Architecture*, vol. 113, p. 101877, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1383762120301569

[32] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5535–5548, 2020.

[33] Z. Wang, H. Wang, Y. Wang, and X. Yang, "Clasrm: a lightweight and secure certificateless aggregate signature scheme with revocation mechanism for 5g-enabled vehicular networks," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[34] Y. Jiang, K. Zhang, Y. Qian, and L. Zhou, "Anonymous and efficient authentication scheme for privacy-preserving distributed learning," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2227–2240, 2022.

[35] K. Sehla, T. M. T. Nguyen, G. Pujolle, and P. B. Velloso, "Resource allocation modes in c-v2x: From lte-v2x to 5g-v2x," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8291–8314, 2022.

[36] H. Liu, X. Luo, H. Liu, and X. Xia, "Merkle tree: A fundamental component of blockchains," in *2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)*, 2021, pp. 556–561.

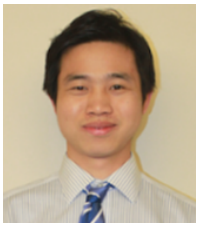
[37] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 283–10 295, 2017.

[38] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of cryptology*, vol. 13, no. 3, pp. 361–396, 2000.
[39] A. Vangala, A. K. Das, A. Mitra, S. K. Das, and Y. Park, "Blockchain-enabled authenticated key agreement scheme for mobile vehicles-assisted precision agricultural iot networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 904–919, 2023.
[40] L. Viganò, "Automated security protocol analysis with the avispa tool," *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61–86, 2006, proceedings of the 21st Annual Conference on Mathematical Foundations of Programming Semantics (MFPS XXI). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1571066106001897
[41] X. Zhang, H. Zhong, J. Cui, I. Bolodurina, and L. Liu, "Lbvp: A lightweight batch verification protocol for fog-based vehicular networks using self-certified public key cryptography," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5519–5533, 2022.
[42] R. Dahlberg, T. Pulls, and R. Peeters, "Efficient sparse merkle trees," in *Secure IT Systems*, B. B. Brumley and J. Röning, Eds. Cham: Springer International Publishing, 2016, pp. 199–215.
[43] *V2X Applications; Part 2: Intersection Collision Risk Warning (ICRW) Application Requirements Specification, document ETSI TS 101 539-2 V1.1.1, Intelligent Transport Systems*, 2018.

**Guanjie Cheng** received the B.S. degree from the School of Computer Science and Technology, Xidian University, Xian, China, in 2018. He is currently working toward the Ph.D. degree with the College of Computer Science and Technology, Zhejiang University, Hangzhou, China. He is currently a visiting Ph.D. in Nanyang Technological University, Singapore. His research interests lie in the fields of privacy computing, blockchain, Internet-of-Things, multi-domain authentication, and trusted management.

**Junqin Huang** received the B.Eng. degree in computer science and technology from University of Electronic Science and Technology of China in 2018. He is currently persuing the Ph.D. degree with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His research interests include Internet of things, blockchain, security.

**Yewei Wang** received the Bachelor's degree in Department of Micro-nano Electronics, Shanghai Jiao Tong University, Shanghai, China. He was a cryptographic development engineer at Wanxiang Blockchain Labs. His research interests lie in secure multi-party computing, privacy computing, blockchain scalability, access control mechanisms, and trusted management.



**Jun Zhao** (Member, IEEE) is currently an Assistant Professor in the School of Computer Science and Engineering (SCSE) at Nanyang Technological University (NTU), Singapore. He received a Ph.D. degree in Electrical and Computer Engineering from Carnegie Mellon University (CMU), Pittsburgh, PA, USA, in May 2015, and a bachelor's degree in Information Engineering from Shanghai Jiao Tong University, China, in June 2010. One of his papers was a finalist for the best student paper award in IEEE International Symposium on Information Theory (ISIT) 2014. His research interests include A.I. and data science, security and privacy, control and learning in communications and networks.

**Linghe Kong** (Senior Member, IEEE) received the B.Eng. degree in automation from Xidian University in 2005, the master's degree in telecommunication from Telecom SudParis in 2007, and the Ph.D. degree in computer science from Shanghai Jiao Tong University in 2013. He is currently a Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University. Before that, he was a Post- Doctoral Researcher with Columbia University, McGill University, and the Singapore University of Technology and Design. His research interests include Internet of things, 5G, blockchain, and mobile computing.

**Shuiguang Deng** (Senior Member, IEEE) is currently a full professor at the College of Computer Science and Technology in Zhejiang University, China, where he received a BS and PhD degree both in Computer Science in 2002 and 2007, respectively. He previously worked at the Massachusetts Institute of Technology in 2014 and Stanford University in 2015 as a visiting scholar. His research interests include Edge Computing, Service Computing, Cloud Computing, Blockchain, and Business Process Management. He serves for the journal IEEE Trans. on Services Computing, Knowledge and Information Systems, Computing, and IET Cyber-Physical Systems: Theory & Applications as an Associate Editor. Up to now, he has published more than 100 papers in journals and refereed conferences. He is a fellow of IET and a senior member of IEEE.

**Xueqiang Yan** is currently a technology expert with the Wireless Technology Lab, Huawei Technologies. He was a member of technical staff at Bell Labs from 2000 to 2004. From 2004 to 2016, he was the director of the Strategy Department, Alcatel-Lucent Shanghai Bell. His current research interests include wireless networking, the Internet of Things, edge AI, future mobile network architecture, network convergence, and evolution.