ABSTRACT In vehicular networks, messages from vehicles are signed before being broadcasted to ensure the authenticity and integrity of the messages. Due to the high mobility of vehicular networks, frequent key updates are often required, which imposes an excessive burden on the key generation process. In this article, we propose a dynamic authentication with conditional privacy-preservation using matrix-based signature generation (DACOP), which is well suited to Vehicle-to-Everything (V2X) networks. The proposed authentication method also provides conditional privacy by utilizing a dynamic pseudo-identity and anonymity of the vehicle. In addition, it can significantly reduce the computation overhead for signature generation. We implemented DACOP and analyzed its computation and communication overhead compared with previous methods. Furthermore, our experimental results using real V2X networks demonstrate that DACOP reduces the computation time by 90% while enhancing the security level by 2 times over previous methods.

INDEX TERMS Vehicle-to-everything (V2X) network, conditional privacy-preservation, matrix-based authentication.

I. INTRODUCTION

Connected-vehicle applications are designed to increase awareness of the driving environment and mitigate traffic accidents through V2X networks which consist of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) network.

Vehicular Ad-hoc Networks (VANETs) are a type of V2X network that implies a self-organizing network. In this article, thus, the two terms VANET and V2X are used interchangeably. To suit the needs for intelligent transportations, V2X allows the vehicles to exchange the emergency alarm, dangers, and traffic information by transmitting basic safety messages (BSMs) periodically, which can avoid traffic accidents and congestions. To ensure the safety of Intelligent Transport Systems (ITS) services, a high level of security procedures is needed to prevent the hackers from corrupting the safety data, transmitting harmful data, and collecting the privacy information of the drivers [1]. The privacy and authenticity of the data are especially eminent issues in the realization of the V2X networks. Most conventional network security methods are not appropriate for the complete protection of vehicular network data, especially for V2X communication among traveling vehicles. Therefore, new methods are needed for message authentication and node anonymity for V2X networks with a large number of fast traveling vehicles.

Most of the previous V2X security methods make use of negotiation to start secure communication with untrusted vehicles. For example, they require frequent message exchanges between the vehicles and the trusted authority for security establishment and key generation. These operations often incur excessive overhead in computation time and communication cost. To address the foregoing problems, our proposed method employs message authentication without the needs for any negotiation and extra message exchanges.

This article proposes a new dynamic authentication method with conditional privacy-preservation (DACOP) using a matrix-based signature generation. It offers substantially...
faster authentication than the conventional methods, which is crucial for V2X message authentication and verification. It can also significantly reduce the communication cost compared with the previous methods. We investigate the impact on packet loss rate, and average packet delay when the vehicle density and vehicle moving speed change. Our main contributions are as follows:

- First, we propose a novel signature generation algorithm based on matrix computations for dynamic authentication with conditional privacy-preservation aimed to solve the critical V2X security problem.
- Second, the proposed method employs the use of dynamic identity for conditional privacy-preservation.
- Third, the proposed matrix-based signature method falls into a class of lattice-based cryptography, it can provide a high level of security. Lattice-based cryptographic constructions provide a promising future for post-quantum cryptography.
- Fourth, we evaluate the practicality and feasibility of the proposed method. We implemented the proposed method on commercial V2X devices and demonstrate that it can significantly reduce the computation and communication costs. Finally, we compare two security algorithms: the proposed method and the IEEE 1609.2 standard.

The rest of this article is organized as follows. A survey of related works is provided in Section II. Section III introduces the system model of the proposed method. Section IV describes the details of the proposed method. The analysis of security level and the proof of its correctness are presented in Section V. The performance evaluation is given in Section VI followed by the conclusions in Section VII.

II. RELATED WORK

For the practical deployment of large-scale V2X networks, many challenges of a dynamic security and privacy problems are yet to be addressed. The conditional privacy-preserving authentication (CPPA) mechanism has been studied by many researchers. It offers message authentication and conditional privacy simultaneously, and thus it is considered as a suitable approach to solving the security and privacy issues in V2X networks. The prior privacy-preserving approaches can be classified into two groups: pseudo certificate-based methods and identity-based methods.

The pseudo certificate-based method is a basic method for vehicular network security and is used by the IEEE 1609.2 standard [16]. In IEEE 1609.2, each vehicle obtains many pseudonym certificates with their key pairs during its registration and uses them for signing messages. Raya and Hubaux [19] proposed a secure vehicular communication scheme using PKI-based certificates. In their security method, each vehicle is preloaded with large numbers of anonymous public/private key pairs and corresponding public key certificates. To enhance security, it updates each public/private key pair with a short lifetime, while utilizing a pseudo-ID within each public key certificate. As a result, it requires larger storage capacity and consequently incurs excessive verification cost, when a public key certificate needs to be verified for every message. In addition, it is difficult to find the adversary’s real identity, since when receiving a fake message, the authority has to perform an exhaustive search of all stored certificates. To address the weaknesses of Raya and Hubaux’s scheme, Lu et al. [28] proposed a new CPPA scheme using anonymous certificates. In this CPPA scheme, a vehicle obtains a temporary anonymous certificate when it passes by a roadside unit (RSU). To satisfy the conditional privacy, each vehicle needs to frequently request a new anonymous certificate from RSU, because it may be easier for the adversary to trace a vehicle if its certificate is used for a long time. However, it is inefficient to keep frequent interactions with RSUs. Therefore, the CPPA scheme of [28] cannot satisfy the requirement of channel efficiency in V2X networks.

To address the certificate management problem described above, identity-based Public Key Cryptography (ID-based PKC) has been introduced to improve the CPPA schemes. In 2008, Zhang et al. [29] proposed an identity-based authentication framework using pairing-based cryptography. In [29], both vehicles and RSUs do not store any secrecy, while sharing only a few parameters. Furthermore, their approach offers batch confirmation for multiple information exchanges. Therefore, the ID-based CPPA scheme of [29] is aimed to overcome the weaknesses of the previous PKI-based CPPA schemes. However, [29] is vulnerable to replay attacks and so cannot satisfy the requirement of non-repudiation. In addition, the bilinear pairing operation is highly time-consuming compared with other recently reported methods.

In 2012, Shim [1] proposed a new ID-based signature scheme and then used it to develop a new efficient conditional privacy-preserving authentication method called CPAS for V2I communication to keep a balance between privacy and traceability. As a result, it achieves anonymous authentication, message integrity, traceability, and unlinkability. The method of [1] achieves conditional privacy-preservation in which each message launched by a vehicle has been mapped to a distinct pseudo-ID and a trusted authority can always retrieve the real identity of the vehicle’s pseudo-ID. In the CPAS scheme, an RSU can simultaneously verify multiple received signatures such that the total verification time can be reduced by 18%, compared with the scheme of [29]. However, Shim’s scheme of [1] incurs heavy computation cost in the signature verification, due to its three multiplication point operations and three pairing operations.

Other conditional privacy-preserving authentication schemes also have been proposed, which enhance the methods of [1] by reducing the computation cost. The high computation cost of the previous works is primarily owing to the complexity of their Map-To-Point and pairing operation. Therefore, for recent methods, the critical problem of reducing the complexity still remains as an unsolved challenge [2]–[10], [26], [27].
In 2015, He et al. [4] addressed the problem of pairing operations of Shim’s CPAS scheme [1] which is one of the most time-consuming operations in cryptographic systems. The work of [4] proposed a new ID-based CPPA scheme for V2X networks based on Schnorr’s signature without using bilinear pairing, which provides the function of batch verification of multiple messages. This method does not use bilinear paring but still supports both mutual authentication and privacy protection simultaneously.

In addition, the signature verification process of [4] requires complex cryptography operations, leading to excessive computation cost, which turns into a network bottleneck in high vehicle density scenarios. Furthermore, in this method, during an attack, although TA can track the true identity of the attacker, TA cannot prevent the attacker from sending additional malicious messages.

To improve the computation cost of [4], Cui et al. proposed ECC-based privacy-preserving schemes with the Chinese Remainder Theorem [35] and Cuckoo Filter [36]. The paper [35] uses fingerprints instead of real identity and password for identity verification, which takes long processing time. The message verification cost of the [35] is almost the same as He et al.’s scheme [4]. Additionally, we found that Cui et al. scheme with Cuckoo Filter [36] is vulnerable to important problems in terms of safety, efficiency, and computational cost.

Li et al. [6] also proposed a novel framework with preservation and repudiation (ACPN) for V2X networks. This method introduced public-key cryptography (PKC) with pseudonym generation, which ensures that legitimate third parties can achieve the non-repudiation of vehicles by obtaining vehicles’ real IDs. In [6], the existing ID-based signature (IBS) scheme and ID-based online/offline signature (IBOOS) scheme are used for the authentication between the RSUs and vehicles, and the authentication among vehicles. However, Li et al.’s method of [6] uses a pairing operation with identity-based cryptography which is very time-consuming.

In 2016, Lo and Tsai [2] proposed a new efficient identity-based batch signature scheme, which is based on a new signature scheme for vehicular sensor networks. Conditional privacy-preserving authentication scheme uses Elliptic curve cryptography (ECC) and general one-way hash function instead of the map-to-point hash function to ensure efficient messages authentication and drivers’ privacy-preservation in V2I and infrastructure-to-vehicle (I2V) communications. The method of [2] reduced the communication cost by 27% in comparison with the method of [4]. However, the size of signed messages for the method [2] is still very large. In addition, the method [2] does not consider the message loss ratio, and thus its message loss ratio tends to degrade for increasing network density.

In 2017, Islam et al. [7] presented a password-based conditional privacy-preserving authentication and group-key generation (PW-CPPA-GKA) protocol for V2X networks. The protocol offers group-key generation and password change facilities for users leaving and joining. This protocol is lightweight, since it is designed without using the bilinear-pairing and elliptic curve. However, since the method of [7] is based on a simplistic hash function, it can provide a limited security level.

Zhang et al. [9] presented a new privacy-preserving authentication protocol for V2X networks. In their protocol, RSU is responsible for constructing a subgroup of the V2X network and managing a private key for vehicles. In 2018, Asaar et al. [10] presented an identity-assisted authentication framework using proxy vehicles. In the same year, Li et al. [11] presented EPA-CPPA: An efficient and secure anonymous conditional privacy-preserving authentication framework for V2X networks [5]. The authors claim that [5] is a secure CPPA scheme and provides both security and privacy for V2X networks. However, these methods suffer from the excessive overhead of bilinear pairing operation. The method of [5] proposed to use biometric and elliptic curve assisted authentication framework. It is not practical, however, since [5] requires that all vehicles should be equipped with tamper-proof biometric devices.

More recent work [3] proposed a more deployable and intelligent conditional privacy-preserving method for vehicular ad-hoc networks. The authors of [3] presented a new ID-based CPPA method for V2X networks based on ECC and bloom filter. The main contribution of the method [3] is that it uses the concept of the bloom filter to identify whether the vehicle is a legitimate or malicious vehicle. However, the method of [3] does not provide proper countermeasures to avoid existing attacks. In addition, group communication in [3] is managed only by the roadside unit.

Recent papers proposed message authentication methods that utilize message-authentication code [8], [32]. For example, Wang et al. [8] proposed a lightweight and efficient strong privacy-preserving (LESPP) authentication scheme that employs a message authentication code (MAC) and symmetric encryption. The method of [8] can reduce both computation and communication overhead. The identity-based signature method is only used for identity generation and this can further reduce communication overhead and avoids certificate management. Wang et al. [32] proposed a Two-Factor Lightweight Privacy-preserving (2FLIP) authentication scheme for VANETs. It introduced the idea of a two-factor authentication technique mainly by utilizing message-authentication-code (MAC) and hash operations for improving the security and privacy of VANETs. However, many researchers do not use the MAC-based methods, because of the certificate and identity management issues. In addition, two or three-factor authentication methods with MAC require additional acknowledgment messages. Furthermore, it may not be possible to apply biometrics with MAC authentication to V2X networks in special scenarios.

In summary, many of the previous methods attempted to reduce the computation time and communication overhead of the secure V2X networks. However, they still have many drawbacks such as the high complexity of the
key negotiation, high cost of security certificate management, excessive transmission overhead, and long delays in negotiations. While many methods cannot ensure security against mutual authentication, forward security, impersonation attack, insider attack, and parallel attack, some of these methods fail in impersonation and untraceable attack.

In this article, we propose a more secure and faster message authentication framework that is dynamic and anonymous, while allowing traceability. Furthermore, our proposed method can considerably reduce the overhead for negotiation and transmission. Our experimental results demonstrate consistently high performance and short processing time under various conditions like a high density of vehicles and a high frequency of beacons.

III. BACKGROUND

In this section, we briefly explain the system model and security requirements of the proposed CPPA solution for V2X networks.

A. NETWORK MODEL

Like most of the previous network architectures [4], the proposed security method employs a two-layer network model. The upper layer of the network model consists of a Trusted Authority (TA) and V2X Application Server (VAS), which is responsible for vehicle registration, authentication, and traffic management issues. The communication between them is conducted through a secure channel. The lower layer of the network model consists of an RSU and vehicles that communicate with each other through wireless link layer standards such as DSRC/IEEE 802.11p. The DSRC stands for Dedicated Short Range Communication. The detailed description of each entity is described as follows.

- **TA** is a trusted system with high computation and storage capabilities such as traffic management authority responsible for vehicle registration, system parameter configuration and security material distribution to registered vehicles and RSUs [38]. It also stores the registration list and other details of RSU and on-board units (OBU). This entity is the only node in the network that can verify the real identity of the vehicles. It is assumed that the TA is fully trusted, and thus it authenticates all the legitimate vehicles and RSUs, while detecting the malicious vehicles.

- **VAS** supports vehicular safety-related applications at the traffic management center. The VAS could communicate with RSUs for providing application support and traffic management.

- **RSU** acts as the medium of communication between the vehicles and the TA. The RSUs are connected to TA via secure communication medium or the internet. Since RSUs are not fully trusted, they must be managed and monitored by the TA and VAS. We assume that all the RSUs are equipped with the DSRC protocol and radio module to transfer data [7].

- **Vehicles** are assumed to be equipped with an OBU device supporting the DSRC protocol. The OBU contains a tamper-proof device and thus its information is protected. By using the DSRC protocol, the OBUs of vehicles can broadcast beacon-messages that carry their location, timestamp, driving status, and traffic condition on the road. The OBU is responsible for maintaining the real identity of the vehicle, secret information, and cryptographic materials to perform cryptographic operations [4], [6]–[8]. Each vehicle equipped with OBU can communicate with nearby vehicles and RSUs.

The typical structure of the V2X network described above is illustrated in Figure 1.

![Figure 1. The network model for V2X.](image-url)

B. SECURITY AND PRIVACY REQUIREMENTS

Both security and privacy are important for secure communications in V2X networks. Many researchers proposed solutions for the following security requirements.

1) **Message authentication and integrity:** In V2X communications, each message is authenticated by the sender to ensure that this message cannot be modified or forged by a malicious adversary. The messages can be verified only by legitimate vehicles and TA.

2) **Identity privacy-preservation:** It must be guaranteed that RSUs and other vehicles cannot extract the vehicle’s real identity. To provide privacy, the real identity of the vehicle is not disclosed in any broadcasted messages. Any attacker or a third party should not be able to learn the vehicle’s real identity by analyzing messages. Only TA can extract the vehicle’s real identity.

3) **Unlinkability:** Adversary vehicles or RSUs must not be able to link any two and more signatures sent by the same vehicle, i.e., they must not be able to trace the vehicle’s action through its messages.

4) **Resistance to various security attacks:** A security method must be able to withstand various attacks such as an impersonation attack, the replay attack, the man-in-the-middle attack, and other attacks.
IV. MATRIX-BASED AUTHENTICATION METHOD

In this section, we describe the proposed ID-based Dynamic Authentication method with Anonymous Conditional Privacy-Preservation (DACOP) using matrix-based cryptography. As demonstrated with simulation results later, the proposed method provides lower computation overhead and a higher level of security than previous methods. The proposed method consists of five phases: (1) offline system initialization and vehicle registration, (2) signing key generation and message signing, (3) verification key computation and message verification, (4) key updates, and (5) vehicle revocation.

The main advantages of the proposed method are as follows:

- It provides simplicity for the implementation under various network scenarios.
- It supports the group-based secure communication requirements of V2X networks.
- It eliminates the need for frequent key negotiation. The initial parameters are installed only in offline setup and system initialization.
- It employs fast matrix arithmetic instead of bilinear pairing which incurs excessive computation overhead.
- It ensures high conditional privacy-preservation of legitimate vehicles.
- It can prevent malicious vehicles from verifying messages signed by legitimate vehicles.
- The using of dynamic identity and changing the key provides the resistance against modern signature learning attacks, with machine learning methods.
- Finally, its computation and communication costs are significantly lower than the previous methods.

Table 1 defines the notations used in this section.

A. SYSTEM INITIALIZATION AND VEHICLE REGISTRATION PHASE

All vehicles' OBUs and RSUs are registered with the trusted authority (TA) via a secure offline protocol. TA is a trusted party with high storage capacity and computing power [38]. The TA is responsible for registering and authenticating the vehicles and RSUs.

![Figure 2. Vehicle tamper proof system.](image)

In the V2X network of our concern, each vehicle is equipped with a tamper-proof software system (TPS), integrated in the OBU. The TPS consists of four modules: (1) system initialization and authentication module, (2) key generation and updating module, (3) message signing module, (4) message verification module; See Figure 2. An OBU with TPS is initiated by the system initialization and authentication module. This module always tests initial system parameters and checks the correctness of received message contents. Therefore, an adversary cannot take advantage of the TPS even if the vehicle is stolen.

1) SYSTEM INITIALIZATION WITH TA

The TA generates system parameters (such as initial prime numbers, hash function indicators, and initial matrix numbers). As an offline operation, the TA preloads them into each vehicle’s tamper-proof system (TPS).

The details of the offline system initialization steps are as follows:

1) Let $F_p$ be the finite field over $p$, where $p$ and $q$ are prime numbers in the range of the finite field. $p$ and $q$ are chosen by TA to satisfy the greatest common divisor $gcd(p, q) = 1$, and to reduce the complexity of the function by using modulo of $p$. The TA generates small and large prime numbers, $p$ and $q$, and selects the matrix size $N$.

2) TA generates a random ternary matrix $G$ of $N \times N$ size, which is a system secret that is provided only to trusted vehicles during the registration phase.

3) TA selects the set of secure hash functions $h$ ($h : \{0, 1\} \rightarrow \mathbb{Z}_q$, $h_1, h_2, h_3, \ldots$ and $h_n$) for different service areas and generates the configuration set. Then, TA preloads the configuration set into each vehicle’s tamper-proof system.

In each vehicle, the selected hash function $h$ is used to calculate message digest $D(m)$ and to generate a pseudo ID of the vehicle (PID) for the predefined service area.

**Table 1. The main symbol definitions.**

| Definition | Description |
|------------|-------------|
| Vehicle<sub>i</sub> | The i-th vehicle |
| TA | The trusted authority |
| TPS | Tamper-proof system |
| $T_i$ | The current timestamp of Vehicle<sub>i</sub> |
| Device ID | The identity of OBU device used for registration with TA |
| RID<sub>i</sub> | The real identity of Vehicle<sub>i</sub> |
| PID<sub>i</sub> | The pseudo-identity of Vehicle<sub>i</sub> in time $T_i$ |
| PWD<sub>i</sub> | The password of Vehicle<sub>i</sub>’s TPS for registration and authentication in TA |
| $m$ | A message to transmit |
| $p$, $q$ | Small and large prime numbers |
| $N$ | A matrix size |
| $K_{\text{sym}}$ | Ternary Seed Matrix [-1, 0, 1], the signing key of Vehicle<sub>i</sub> |
| $G$ | A random ternary matrix of size $N \times N$ generated by TA |
| $R$ | A random ternary matrix of size $N \times N$ generated by each vehicle’s TPS |
| $K_{\text{ver}}$ | A key for verification |
| $h$ | A set of secure one-way hash functions, $h : \{0, 1\} \rightarrow \mathbb{Z}_q$ |
| $D(m)$ | A message digest, the result of the hashing message $m$. |
| $s$ | A signature |
The proposed method uses $n$ hash functions for $n$ regions of the V2X network, which together with different signing keys per vehicle can further strengthen the security.

2) VEHICLE REGISTRATION WITH TA

The TA registers each vehicle in the following steps using secure offline communication:

1) Each vehicle submits to TA its Device ID and vehicle information.
2) TA assigns a real identity $RID_i$ and a password $PWD_i$ to each vehicle $V_i$. Then $V_i$ pre-loads $\{RID_i, PWD_i\}$ into its tamper-proof system (TPS) in $V_i$’s OBU.
3) TA loads all system parameters $\{p, q, N, h, G\}$ to vehicles and RSUs as illustrated by Figure 3.

![Vehicle registration procedure.](image)

After registration, the individual vehicle initializes its TPS and keeps system parameters $\{p, q, N, h, G\}$ in TPS, which then allows the OBU to join secure V2X communication.

![Signed message broadcasting with DSRC transmission in and out of RSU coverage.](image)

B. SIGNING KEY GENERATION AND MESSAGE SIGNING PHASE

In vehicular communication, when a vehicle generates periodic safety messages like BSM (Basic Safety Message) of DSRC/IEEE1609, the message is signed before broadcast. Figure 4 illustrates an example V2X network consisting of vehicles (OBU s) and an RSU, where the transmission range of sender vehicles is indicated by dotted circles. In this phase, the vehicle’s tamper-proof system (TPS) inside OBU performs message signing operation. For every message, TPS first generates a private (signing) key and then signs the message using the digital signature algorithm with the private key.

1) PRIVATE KEY GENERATION PHASE

The key generation module in TPS generates ternary matrix $K_{sign}$ of size $N \times N$, which is used as a singing key $K_{signi}$ of Vehicle$_i$.

2) MESSAGE SIGNING PHASE

TPS signs a message in the following steps:

1) The Message signing module of TPS in the vehicle computes the message digest of message $m$ as the result of the hash function ($h$): $D(m_i) = h(m_i)$. The message digest is represented in a matrix form $D(N \times N)$ for signature generation.
2) The module computes the signatures as follows:

$$s_i = K_{signi} \times (D(m_i) + R \times q)(\mod q).$$

Here, $R$ is a random ternary matrix of size $N \times N$ generated by each vehicle’s TPS to strengthen the security. $R$ has the same size as matrix $K_{signi}$. $R$ is only used for signature generation. The correctness of (1) is proved by (7) and (8) in the next section. The receivers can extract $K_{ver}$ using only $p, q, G$, so the receivers can verify the signed message without requiring $R$.
3) Authentication module generates a pseudo ID of Vehicle$_i$ - PID$_i$ by using (2):

$$PID_i = (K_{signi}^{-1} \times D(m_i)).$$

4) Then, vehicle $V_i$ broadcasts a message of format $\{m_i, T_i, PID_i, s_i\}$ to other vehicles and RSUs. Figure 5 depicts the signed message format.

![Signed message format from IEEE 1609.2 standard.](image)

C. VERIFICATION KEY COMPUTATION AND MESSAGE VERIFICATION PHASE

When each vehicle receives a message $\{m_i, T_i, PID_i, s_i\}$ from a sender vehicle $V_i$ in the transmission ranges, the receiver verifies the message in its verification module as follows before accepting the message.

In the proposed method, the receiver checks the validity of the received message through the traditional time-based verification process. Verifying the received message by the time checks whether it is a fresh message or is replayed by an attacker within the time threshold. If the message is suspected as being replayed, the verifier rejects the message.

Let $V_j$ denotes the receiver vehicle, and $m'_i$ indicates the received message from sender $V_i$. Note that in subsection B, the original message transmitted by $V_i$ is defined by $m_i$.

1) VERIFICATION KEY COMPUTATION PHASE

The verification key is computed and used by all receivers $V_j$’s within the transmission range of the sender $V_i$.

1) Receiver $V_j$ computes the message digest $D'(m'_i)$ from the received message $m_i$ by using (3).

$$D'(m'_i) = h(m'_i).$$

VOLUME 8, 2020
2) Receiver $V_j$ computes $K_{\text{sign}}\times_q$ by (4), which is $(K_{\text{sign}})^{-1} \mod q$.

$$K_{\text{sign}}\times_q = P\text{ID}_i/D(m'_i). \quad (4)$$

3) Receiver $V_j$ computes verification key $K_{\text{ver}}$ signature verification using (5) with $K_{\text{sign}}, q$ and other system parameters.

$$K_{\text{ver}} = (K_{\text{sign}} + p \times G). \quad (5)$$

Here, $G$ is a random ternary matrix generated by TA as explained above in the initialization phase. $G$ is a common matrix for registered vehicles and RSUs.

2) MESSAGE VERIFICATION PHASE

1) To retrieve the original digest, Receiver $V_j$ decrypts signature $s_i$ in the received message by using (6) with verification key $K_{\text{ver}}$:

$$D(m_i) = ((K_{\text{ver}} \times S_i) \mod q) \mod p. \quad (6)$$

2) Receiver $V_j$ compares $D'$ ($m'_i$) calculated by (3) with original digest $D$ ($m_i$) retrieved by (6). If they match, receiver $V_j$ accepts message $m'_i$. Otherwise, $V_j$ rejects $m'_i$. Here, both the calculated digest $D'$ ($m'_i$) and the original digest $D$ ($m_i$) are represented in a form of an $N \times N$ matrix.

D. KEY UPDATES

The signing key $K_{\text{sign}}$ is generated periodically by TPS of the vehicle and used for a short time to increase the security level. On the other hand, the verification key $K_{\text{ver}}$ is recalculated with every message, since the hash result is different.

The key advantage of the proposed method is that the key update is carried out in each sender vehicle without the need for communication with RSUs and TA.

In the proposed method, therefore, the signing key generation and update processes impose virtually zero overhead of message exchange with TA. When a legitimate vehicle finds that its signing key is expired or compromised, it updates the key $K_{\text{sign}}$ or requests TA to update the initial system parameters.

E. VEHICLE REVOCATION

Only TA has the privilege of vehicle registration or revocation of old registration information. The vehicle revocation process is organized by TA upon the request from vehicle $V_i$ with an encrypted channel or secure wireline. When the vehicle sends a request to TA for revocation, TA asks for the device ID and registration details of $V_i$. After verifying the vehicle details, TA requests $V_i$ to encrypt and send the real identity and registration password $\{\text{RID}_i, \text{PWD}_i\}$ of vehicle $V_i$. Then vehicle $V_i$ sends to TA a registration ID and password in encrypted form. After this two-step verification, TA deletes old system parameters and generates new system parameters $\{p, q, N, h, G\}$ for $V_i$. As a result, adversary vehicles cannot generate signed messages with old parameters, even if the secret information of $V_i$ was compromised by the adversary. In this way, the system parameters are revoked and updated periodically. So, the adversary vehicles cannot attack the authentication and privacy of the V2X messages.

V. SECURITY ANALYSIS

In this section, we analyze the correctness and the security and privacy capability of the proposed DACOP method with a matrix-based message signing algorithm for V2X networks.

A. CORRECTNESS PROOF

To show the correctness of the proposed signature algorithm, we prove the correctness of (6), which is the message verification process in the receiver vehicle.

In the signature generation process of (1), a random matrix $R$ is added to the message digest value, which is then multiplied by signing key $K_{\text{sign}}$. It is exponentially complex to find the signing key $K_{\text{sign}}$, even if the message digest value is known by the receiver after signature decryption. Therefore, the proposed algorithm is still highly secure, even though the values of $N, p, q, h$ are exposed to all verifier vehicles.

When a verifier receives a broadcast message, the verifier computes verification key $K_{\text{ver}}$, decrypts signature $s_i$, and compares $D'$ with this verification key. If the verification key decrypts the message correctly, the algorithm is proved. The correctness of the proposed algorithm is proved by (7) and (8).

For proof, we put the equations (5) and (1) into (6) and calculate the equation (7).

$$D(m_i) = ((K_{\text{ver}} \times S_i) \mod q) \mod p$$

$$= [((K_{\text{sign}} + p \times G) \times (K_{\text{sign}} \times (D(m_i) + R \times q)))) \times q) \mod p$$

$$= [(K_{\text{sign}} + K_{\text{sign}} \times (D(m_i) + R \times q) \mod q + K_{\text{sign}} \times (p \times G) \times (D(m_i) + R \times q) \mod q]] \mod p$$

$$= (K_{\text{sign}} \times (p \times G) \times (D(m_i) + R \times q))) \mod p$$

Due to the equalities of $K_{\text{sign}} \times K_{\text{sign}} = 1, (R \times q) \mod q = 0$, and $(p^* G^* K_{\text{sign}}) \times R \times q \mod q = 0$, we can derive Eq. (8).

$$D(m_i) = [(K_{\text{sign}} \times K_{\text{sign}}(D(m_i)) + 0)$$

$$+(K_{\text{sign}} \times (p \times G) \times (D(m_i) + 0))] \mod p$$

$$= 1 \times D(m_i) + 0 = D(m_i). \quad (8)$$

Here, since $(p \times G \times K_{\text{sign}}) \mod q = 0$, we derived (8).

With (7) and (8), the correctness of (6) is proven, and so is the correctness of the proposed signature generation and verification algorithm.

B. SECURITY AND PRIVACY ANALYSIS

In this section, we prove that the proposed method satisfies the following security and privacy requirements for V2X networks.

1. Message authentication and integrity: According to the VANET standard [16], message authentication is one of the main security requirements for reliable communication. An attacker cannot forge a valid message
in the proposed method, even if it calculates the message digest. A message can be authenticated by generating a signature at the transmitter, while at the receiver verifying the signature container $s$ that is not simply calculated from the hash result but is calculated from 512-bit hash data and 64-bit matrix decryption.

2. **Identity privacy-preservation:** In the proposed method, the real identity of the vehicle is hidden and not used in the message signing process. A $PID$ of the vehicle is temporary and gets changed for every message using equation (2). $PIDs$ are not extracted from the vehicle’s real identity. Only TA can track and retrieve the vehicle’s real identity by requesting the real identity $RID$ and password $PWD$ in a secure method with the “Vehicle Revocation phase”. Therefore, the proposed method DACOP preserves the privacy of vehicle identity.

3. **Traceability:** In the proposed method, only the TA can trace the real identity $RID_i$ of the vehicle $V_i$ and conduct the “Vehicle revocation phase” as discussed above. It is not possible for a third party (vehicle/RSU/attacker) to extract the real identity of vehicles just by analyzing their messages. If a malicious vehicle sends a bogus message to the TA pretending to be a legitimate vehicle, then the TA can identify it by revealing the identity of the suspected vehicle. Consequently, DACOP allows the TA for complete traceability, while it prevents traceability entirely from any vehicles.

4. **Unlinkability:** The signature generation, different message content, a digest computation, and the private keys of DACOP ensure unlinkability. DACOP changes the $PID$ of each vehicle for every message to achieve both message and user unlinkability.

   - **Message unlinkability:** Assume that an adversary vehicle tries to learn the difference between two messages $m$ and $m'$ that are broadcasted from the same vehicle. The adversary, however, cannot retrieve the PID, because of each vehicle updates for every message the signing key and PID producing unpredictable hashing result. The unlinkability is ensured by generating signatures of two messages using different $PIDs$. Therefore, the proposed method enables comprehensive message unlinkability.

   - **User unlinkability:** It is impossible for an attacker to retrieve the real ID of vehicles, since PID in every message is not related to the real ID.

5. **Resistance to message stealing and privacy attacks:** As described above, the proposed method could withstand the following attacks that are considered critical concerned with V2X networks.

   - **Impersonation attack:** DACOP protects the network from the impersonation of the vehicle. For an attacker to impersonate $V_i$ with respect to the TA, the TA requires to register $DeviceID$, $RID_i$ and an individual password of vehicle $V_i$. These parameters are secret, only known to $V_i$ and TA. Even if the attacker extracts the previous $PID$ of $V_i$, the attacker cannot compute the correct authentication message, since the $PID$ changes for every message.

   - **Replay attack:** The replay attack occurs, when a malicious vehicle receives an authentication message of the previous session and retransmits it in the current session to impersonate the vehicle. The timestamp $T_i$ is included in the message. The verifiers could detect a replay attack when $T_i$ is outdated. If the timestamp is changed by the attacker, the receiver vehicle can detect the change by signature verification and report this to the TA by a notification message.

   - **Man-in-the-middle attack:** Based on the above analysis of the message authentication and integrity, DACOP can provide authentication between the sender and the receiver. Thus, DACOP can prevent a man-in-the-middle attack.

   - **Message modification attack:** DACOP calculates a digital signature $\{PID_i, s_i\}$ for each message $\{m, T_i\}$. Any modification of the message leads to a verification result of mismatch. Any vehicle can detect the modification of the message $\{m_i, T_i, PID_i, s_i\}$ by checking the result of verification. Therefore, DACOP can protect the messages from the message modification attack.

In addition, DACOP does not require any certificates for message signing and verification. Each vehicle or RSU only needs to securely maintain its system and registration parameters $(p, q, N, h, G)$, $DeviceID$, $RID_i$, and $PWD_i$, which are generated by TA during the initial registration. Therefore, the proposed method satisfies complete privacy and security requirements without the need for complex certificate management procedures.

**VI. PERFORMANCE EVALUATION**

In this section, we analyze the performance of the proposed DACOP method for V2X networks based on Matrix-based cryptography. We compare both the computation cost and communication cost of DACOP with other previous methods.

**A. IMPLEMENTATION AND SIMULATION PLATFORM**

To make a fair comparison of the computation cost, we implemented both the proposed DACOP method and the previous methods including Shim [1], He et al. [4], Pulagara and Alphonse [3], Li et al. [11], Mundhe et al. [33] under the same NS-3 network simulation framework. All implemented methods are simulated using a PC with 2.5GHz Intel Core i5, 8G RAM, and Ubuntu Linux 18.04. In the proposed method and [33], we use lattice-based public-key cryptography with a matrix-based signature generation method using the Euclidean Division Theory of polynomials. In our case, the size of $p$ and $q$ is 16 bits, the matrix size is $8 \times 8$ with
a security level comparable to 192 bits. For the performance comparison in this section, we chose a block size of 512 bits.

### B. COMPUTATION COST ANALYSIS

For analyzing computation cost, we define the notations of cryptographic operations that comprise the major computation cost of the proposed DACOP:

- $T_{\text{mod}}$: The execution time for calculating the modular operation;
- $T_{\text{MM}}$: The execution time for multiplying two matrices;
- $T_{\text{NumM}}$: The execution time for multiplying a number and matrix;
- $T_{\text{add}}$: The execution time for adding two matrices;
- $T_{\text{hash}}$: Time to compute a one-way hash operation.

Table 2 shows the computation time of cryptographic operations from the simulation.

| Operation | Execution time (nanoseconds) |
|-----------|-----------------------------|
| $T_{\text{mod}}$ | 750 |
| $T_{\text{MM}}$ | 1650 |
| $T_{\text{NumM}}$ | 500 |
| $T_{\text{add}}$ | 500 |
| $T_{\text{hash}}$ | 300 |

Now, we compare our proposed method with existing CPPA methods for V2X networks. We chose the schemes based on the ECC, bilinear pairing, and lattice-based cryptography for comparison. Here, bilinear pairing-based ID-based CPPA schemes for V2X use a bilinear pairing. The bilinear pairing is an operation of mapping of elements from two cryptographic groups to a third group, with an explanation $\bar{e} : \bar{G}_1 \times \bar{G}_1 \rightarrow \bar{G}_T$ to achieve a security level comparable to 80 bits. Here $\bar{G}_1$ is an additive group generated by a point $\bar{P}$ with the order $\bar{q}$ on the super singular elliptic curve $\bar{E}$: $y^2 = x^3 + x \mod \bar{p}$ with an embedding degree of 2. $\bar{p}$ is a 512-bit prime number, while $\bar{q}$ is a 160-bit Solinas prime number, so that the equation $\bar{p} + 1 = 12\bar{q}r$ holds. For previous ECC-based ID-based CPPA schemes for VANETs, we use an additive group $G$ generated by a point $P$ with the order $q$ on a non-singular elliptic curve $E : y^2 = x^3 + ax + b \mod p$ to achieve the security level of 80 bits, where $p, q$ are two 160-bit prime numbers and $a, b \in \mathbb{Z}_p^*$. For the comparison with other methods, we present execution times of different operations that are used in ECC based schemes [1], [3], [4], [11], [22]:

- $T_{\text{bp}}$: The execution time of a pairing operation $(S, T)$, where $S, T \in G$ (an additive group) $\approx 3.65 \text{ ms}$.
- $T_{\text{sm-ecc}}$: The execution time of a scale multiplication operation related to ECC $\approx 0.385 \text{ ms}$.
- $T_{\text{pa-ecc}}$: The execution time of a point addition operation related to ECC $\approx 0.0018 \text{ ms}$.

The performance evaluation of methods in terms of the execution time consumed to generate and verify authenticated messages is shown in Table 3 and Table 4.

| Scheme | Total computation cost | Total Execution time (milliseconds) |
|--------|------------------------|------------------------------------|
| Shim [1] | $3T_{\text{bp}} + T_{\text{hash}}$ | 4.5005 |
| He et al. [4] | $3T_{\text{sm-ecc}} + 3T_{\text{hash}}$ | 1.1565 |
| Pulagara et al. [3] | $T_{\text{sm-ecc}} + 6T_{\text{hash}}$ | 0.388 |
| Li et al. [11] | $T_{\text{sm-ecc}} + 2T_{\text{hash}}$ | 0.386 |
| Mundhe et al. [33] | $T_{\text{hash}} + \pi T_{\text{NumM}} + 6T_{\text{add}}$ | 0.0254 |
| The proposed method | $T_{\text{hash}} + T_{\text{NumM}} + T_{\text{add}} + T_{\text{MM}} + T_{\text{mod}}$ | 0.0037 |

*(n* - the number of vehicles. Here, we used a minimum number of vehicles used in simulation, n=10.)*

| Scheme | Total computation cost | Total Execution time (milliseconds) |
|--------|------------------------|------------------------------------|
| Shim [1] | $3T_{\text{bp}} + 2T_{\text{sm-bp}} + T_{\text{pa-bp}} + 2T_{\text{hash}}$ | 13.9575 |
| He et al. [4] | $3T_{\text{sm-ecc}} + 2T_{\text{hash}} + 2T_{\text{pa-ecc}} + T_{\text{hash}}$ | 1.1596 |
| Pulagara et al. [3] | $T_{\text{sm-ecc}} + 4T_{\text{hash}}$ | 0.387 |
| Li et al. [11] | $4T_{\text{sm-ecc}} + T_{\text{pa-ecc}} + 2T_{\text{hash}}$ | 1.5428 |
| Mundhe et al. [33] | $T_{\text{hash}} + \pi T_{\text{NumM}} + 6T_{\text{mod}}$ | 0.0243 |
| The proposed method | $T_{\text{hash}} + T_{\text{NumM}} + 2T_{\text{mod}}$ | 0.00345 |

From Tables 3 and 4, it is clear that the proposed method can substantially reduce the computation cost for message authentication and verification compared to other methods.

The computation cost results of compared methods are shown in Figure 6, which is obtained using a message of one block (512 bit) with NS3 simulator.

Figure 6 shows that the proposed method achieves computation reduction up to 90 times in message signing and 200 times in verification compared with the method of Shim [1]. The proposed method does not require a key generation phase, negotiation phase, or bilinear pairing operations, which can impose significant overhead. In addition, our method provides a higher security level compared to other works.

While the previous methods [1], [3], [4] and [11] are designed to achieve the security level of 80 bits, our method
ensures a security level of 192 bits. In addition to the reduction in computation cost, we enhanced the security level by 2 times. Therefore, the proposed method can be considered as a fast but highly secure privacy-preservation and message authentication method well suited to V2X networks.

C. COMMUNICATION COST ANALYSIS

We analyze the communication overhead of the proposed method and compare the overhead with 5 different previous methods, which is summarized in Table 5. The overhead of each method is described as follows.

| Methods                     | Cryptographic overhead (bytes) |
|-----------------------------|-------------------------------|
| IEEE standard [16]          | 181                           |
| Shim [1]                    | 105                           |
| He et al. [4]               | 144                           |
| Li et al. [11]              | 144                           |
| Alazzawi et al. [26]        | 108                           |
| The proposed method         | 52                            |

As mentioned in the previous subsection, the size of $\bar{p}$ is 64 bytes, meaning that the size of each element in $G_1$ is 128 bytes, and the size of $p$ is 20 bytes, meaning that the size of each element in $G$ is 40 bytes respectively. Besides, the size of the general hash output is 20 bytes (the hash output of the proposed method is 32 bytes), while the timestamp is 4 bytes.

Based on the IEEE standard draft [16] for V2X network security, a message of size 67-200 bytes generated from an OBU or an RSU is encapsulated to secure the communication between vehicles. To authenticate a message for message integrity, the sender signs the messages with their private keys. The signed message contains one byte for protocol version, one byte for type, 67-200 bytes for the original message, 125 bytes for a certificate, and 56 bytes for ECDSA signature, as shown in Figure 7.

In summary, the proposed DACOP method incurs significantly lower overhead in packet size and consequently requires much lower compared with the IEEE standard for V2X network security and other previous methods.

D. NETWORK SIMULATION ANALYSIS

Here, we evaluate our method in the aspect of efficiency and network performance with simulation. We conducted the simulations on a desktop PC with Intel(R) Core i5 CPU with 2.5GHz and 8GB RAM with a Linux platform.

In the V2X network environment, we consider end-to-end delay and message loss ratio as performance metrics. We tested with messages using conventional beacons and beacons signed with the proposed method, respectively. We implemented the proposed DACOP method using the ID-based infrastructure. The overhead was reduced by 76 bytes. Other papers [2], [24] also adopted the reduced message format from Shim’s scheme; See Figure 8. In an optimized format [2], the overhead was reduced to 105 bytes, by using Type ID of 1 byte, Message ID of 1 byte, and Payload (Message) of 67 bytes. Therefore, the packet format of [2] is often employed by many recent papers. Here, the Type ID and Message ID are a part of the IEEE1609/WAVE protocol.

Our proposed DACOP method can further reduce the overhead of the packet length by using the proposed compact signature and pseudo-identity; See Figure 9. As a result, the total minimal payload size is minimized to 54 bytes.
network simulator NS3. We built various V2X network scenarios and measured the network performance.

We simulated a highway traffic scenario with a changeable vehicle density and speed, which provide realistic test scenarios for the end-to-end delay and message loss ratio. The network performance evaluation is conducted with a various vehicle speed of 5-50m/s, and a vehicle density of 10-80 vehicles with acceleration 5m/s². IEEE 802.11p module in NS3 is used to simulate the medium access control layer transmission protocol of WAVE standard over an idle channel. The bandwidth of the channel was configured at 6 Mb/s. The simulation parameters are shown in Table 6.

The average message delay (avgD) and average loss ratio (avgLR) are considered in this simulation. The avgD is expressed by (9).

\[
avgD = \frac{1}{N_A \cdot M_{sent,n} \cdot K_n} \sum_{i=1}^{N} \sum_{m=1}^{M_{sent,n}} \sum_{k=1}^{K_n} (T_{i,m}^{\text{sign}} + T_{i,m,k}^{\text{transmission}} + T_{i,m,k}^{\text{verify}} \cdot (L_{i,m,k} + 1)).
\]

Here, \(N_A\) represents the number of vehicles in the network area \(A\), \(M_{sent,n}\) is the number of messages sent by vehicle \(i\), and \(K_n\) indicates the number of adjacent vehicles within the one-hop communication range of vehicle \(i\). \(T_{i,m}^{\text{sign}}\) is the time taken by vehicle \(i\) for signing message \(m\), \(T_{i,m,k}^{\text{transmission}}\) represents the message \(m\) sent by vehicle \(i\) and received by vehicle \(k\), and \(T_{i,m,k}^{\text{verify}}\) is the verifying time of the message \(m\), which is sent by vehicle \(i\) and received by vehicle \(k\). \(L_{i,m,k}\) is the length of the message queue in the vehicle \(k\) that stores message \(m\) sent by vehicle \(i\).

To compare the efficiency of the proposed method in vehicular communication, we conducted simulation measurements with three methods: the proposed method, He et al. [4], and Li et al. [11]. In simulation, the number of vehicles varies from 10 to 80 vehicles per network area and the average speed of vehicles is approximately 20 m/s (72 km/h).

Table 6. Simulation setup.

| Parameters               | Values                      |
|--------------------------|-----------------------------|
| Simulation environment   | NS3.29                      |
| MAC Protocol             | 802.11p(WAVE)               |
| Wi-Fi Physical Data Rate | OfdmRate6MbpsBW10MHz         |
| Transmission Range       | 250m                        |
| Broadcast interval       | 0.1s                        |
| Vehicle density          | 10-100 vehicles             |
| Vehicle speed            | 5-50m/s                     |
| Mobility Model           | Highway                     |
| Propagation loss model   | Long Distance Propagation Loss Model |
| Simulation area          | 50x1000 m                   |
| Simulation time          | 100 sec                     |
| Standard beacon size     | 100 bytes                   |
| Signed message size      | 152 bytes                   |

![FIGURE 10. Impact of vehicle density on the average message delay.](image1)

Figure 10 illustrates the performance of \(avgD\) over the number of vehicles. The \(avgD\) increases slightly with increasing traffic density for all three methods. While the \(avgD\) values for He et al. [4] and Li et al. [11] are 4.137 ms and 5.286 ms, respectively, for a vehicle density of 10, the proposed method provides an \(avgD\) of only 0.67ms, a substantial reduction. Therefore, the \(avgD\) of the proposed method is up to 7 times lower than [4], [11] and thus hardly affects the communication performance.

![FIGURE 11. Impact of vehicle moving speed on the average message delay.](image2)

Figure 11 shows the relationship between \(avgD\) and the speed of vehicles. We can observe that the speed of vehicles has little impact on the \(avgD\) performance.

The average message loss ratio (avgLR) is defined by the number of dropped messages over the total number of received messages in each vehicle. Here, we consider the message loss caused only by the computation load of the security protocol rather than the wireless transmission channel. Such message loss is observed, when the queue is full at the receiver vehicle because the message arrival rate is higher than the message verification rate. We used an optimized buffer size \(L_{i,m,k}\) in \(avgD\) calculation of the proposed method considering the worst-case scenarios (up to 250 vehicles are in communication range) [30]. Hence, the \(avgLR\) for the proposed method remains nearly 0 regardless of the vehicle density.

Figure 12 illustrates the average message loss ratio over the number of vehicles. In Figure 12, for a vehicle density of 50 vehicles, the \(avgLR\) of [4], [11] and the proposed method remains nearly 0. As the vehicle density further increases, the \(avgLR\) starts increasing. For a vehicle density...
of 140 vehicles, Figure 12 shows an $avgLR$ of 57% for [11] and 43% for [4]. In contrast, the $avgLR$ of the proposed method remains zero until the vehicle density grows up to 140 vehicles. Such a significantly low loss ratio of the proposed method is attributed to the low computation overhead and low message overhead of the proposed method.

The above simulation results demonstrate that the proposed method can significantly reduce both computation and network overhead without compromising the security level.

### E. NETWORK MEASUREMENT EXPERIMENTS

To further validate and evaluate the proposed DACOP method in a real V2X network with commercial V2X devices, we implemented our proposed protocol in a C program on Cohda Wireless’s On-Board Unit, MK5 module. See Figure 13 for a MK5 V2X device used in the experiment. We conducted experiments with a real vehicular network consisting of 4 MK5 OBU modules, which is illustrated in Figure 13.

The OBU device is configured as follows:
- IEEE 802.11p radio with a carrier frequency of 5.9GHz and a signal bandwidth of 10MHz;
- Global Navigation Satellite System (GNSS) for synchronization and position information;
- Integrated Hardware Security Module for acceleration;
- IEEE 1609.2 Protocol Stack running over Linux;
- Supports DSRC (IEEE 802.11p) with PHY data rate configured for 6 Mbps;
- IEEE 1609.2 Security protocol for authentication.

In the test network with four OBU modules illustrated in Figure 13, each module generates a BSM message in every 100ms.

The experiments investigate the number of signed and verified messages with respect to the consumed time.

#### TABLE 7. Computation time measurement of message authentication for a message of 100 bytes.

| Implementations         | Signing Time (milliseconds) | Verification Time (milliseconds) |
|-------------------------|-----------------------------|----------------------------------|
| The IEEE 1609.2 standard (software) | 29.3                        | 28.5                             |
| The IEEE 1609.2 standard (hardware) | 5.75                        | 6.12                             |
| The proposed method     | <0.05                       | ≈ 0.075                          |

Table 7 first shows the computation time of signing and verification of one message of 100 bytes, respectively, is 29.3ms and 28.5ms for the IEEE 1609.2 standard with the software security module. We then turned on the HSM module called SXA1700 and measured the maximum performance of the IEEE 1609.2 standard [17], which provides about 5 times improvement in signing and verifying time as shown in Table 7.

In contrast, Table 7 shows that for the proposed method, it takes only 50 and 75 microseconds, respectively, for singing and verifying the same message.

Therefore, our experiment demonstrated that our proposed DACOP method implemented only in software outperforms the IEEE 1609.2 standard running on the HSM accelerator by about 100 times.

Figure 14 illustrates the verification computation time of messages with various sizes. We can observe that the proposed method achieves 285 times shorter verification time than the IEEE 1609.2 standard with the software security module for the messages of size ranging from 100 bytes to 2000 bytes. The computation time increases over the growing message size for both the proposed method and IEEE 1609.2 are attributed to the hash calculation time. The majority of the computation time difference owes to the substantially faster algorithm of the proposed authentication method regardless of the message size.

Table 8 compares the end-to-end communication delay for the proposed method and the IEEE 1609.2 standard, which includes the transmission time, and the delays for the transmit and receive buffers as well as the signing and verifying process delay. In Table 8, while the IEEE 1609.2 standard incurs a delay of 60ms, the proposed method has a delay of only 4~5 ms, which is 12 times improvement.

The measurement experiments presented above show that the proposed method is substantially faster authentication process time and less communication overhead than the IEEE 1609.2 standard. Therefore, the proposed method is an effective approach to solving V2X message authentication problems especially for congested city areas with ever growing network density.
H. Aliev, H.-W. Kim: Matrix-Based Dynamic Authentication With Conditional Privacy-Preservation for Vehicular Network Security

FIGURE 14. Computation time of message verification with the different size: (a) The computation time of the proposed method and the IEEE 1609.2 standard. (b) The computation time of the IEEE 1609.2 standard in detailed scale. (c) The computation time of the proposed method in detailed scale.

TABLE 8. Measurement delay of end-to-end communication for a V2V message.

| IMPLEMENTATIONS      | Communication latency with security support (milliseconds) |
|----------------------|----------------------------------------------------------|
| The IEEE 1609.2 standard (software) | ≈ 60                                                     |
| The proposed method   | ≈ 4.5                                                    |

VII. CONCLUSION

This article presents a novel ID-based Conditional Privacy-Preserving authentication method named DACOP for V2X networks based on matrix-based cryptography. DACOP provides a fast-dynamic algorithm for anonymous authentication of V2X messages, which is especially effective for V2V communication scenarios. The DACOP authentication method enhances the security level and privacy for V2X communications in intelligent transportation systems. DACOP provides a strong authentication without the needs for key generation and negotiation processes.

We implemented the proposed method in a network simulator as well as actual V2X networks with commercial OBU devices. Our extensive experimental results demonstrate that DACOP substantially reduces the authentication processing time and communication overhead, and consequently, it significantly reduces the message loss compared with the IEEE 1609.2 standard. Therefore, the proposed method provides an effective solution to faster and anonymous message authentication for V2X networks with an enhanced security level.

In future work, we plan to extend the proposed method to various application scenarios of V2X communications. We also plan to enhance the proposed method by applying machine learning methods in multi-hop communication and RSU/5G infrastructure [37] and demonstrate the resistance against modern signature learning attacks.

REFERENCES

[1] K. A. Shim, “CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks,” IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1874–1883, May 2012. Accessed: May 2020, doi: 10.1109/TVT.2012.2186992.
[2] N.-W. Lo and J.-L. Tsai, “An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings,” IEEE Trans. Intell. Transp. Syst., vol. 17, no. 5, pp. 1319–1328, May 2016. Accessed: May 2020, doi: 10.1109/TITS.2015.2502322.
[3] S. B. Pulagara and P. J. A. Alphonse, “An intelligent and robust conditional privacy preserving authentication and group-key management scheme for vehicular ad hoc networks using elliptic curve cryptosystem,” Concurrency Comput., Pract. Exper., p. e5153, Feb. 2019. Accessed: May 10, 2020, doi: 10.1002/cpe.5153.
[4] D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 12, pp. 2681–2691, Dec. 2015. Accessed: May 10, 2020, doi: 10.1109/TIFS.2015.2473820.
[5] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, and M. K. Khan, “SEBAP: A secure and efficient biometric-aided-assisted authentication protocol using ECC for vehicular cloud computing,” Int. J. Commun. Syst., p. e4103, Jul. 2019. Accessed: May 10, 2020, doi: 10.1002/dac.e4103.
[6] J. Li, H. Lu, and M. Guizani, “ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 4, pp. 938–948, Apr. 2015. Accessed: May 10, 2020, doi: 10.1109/TPDS.2014.2308215.
[7] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, “A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs,” Future Gen. Electron. Comput. Syst., vol. 84, pp. 216–227, Jul. 2018.
[8] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, “LESP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication,” Computing, vol. 98, no. 7, pp. 685–708, Jul. 2016. Accessed: May 10, 2020, doi: 10.1007/s00607-014-0393-x.
[9] J. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, “Distributed aggregate privacy-preserving authentication in VANETs,” IEEE Trans. Intell. Transp. Syst., vol. 18, no. 3, pp. 516–526, Mar. 2017. Accessed: May 12, 2020, doi: 10.1109/TITS.2016.2579162.
[10] M. R. Assar, M. Salmassiadeh, W. Susilo, and A. Majidi, “A secure and efficient authentication technique for vehicular ad-hoc networks,” IEEE Trans. Veh. Technol., vol. 67, no. 6, pp. 5409–5423, Jun. 2018. Accessed: May 25, 2020, doi: 10.1109/TVT.2018.2822768.
[11] J. Li, K.-K.-R. Choo, W. Zhang, S. Kumari, J. J. P. C. Rodrigues, M. K. Khan, and D. Hogrefe, “EPA-CPPA: A efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” Veh. Commun., vol. 13, pp. 104–113, Jul. 2018. Accessed: May 25, 2020, doi: 10.1016/j.vehcom.2018.07.001.

[12] H. Lu and J. Li, “Privacy-preserving authentication schemes for vehicular ad hoc networks: A survey,” Wireless Commun. Mobile Comput., vol. 16, no. 6, pp. 643–655, Apr. 2016. Accessed: May 25, 2020, doi: 10.1002/wcm.2538.

[13] X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GISIS: A secure and privacy-preserving protocol for vehicular communications,” IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007. Accessed: May 25, 2020, doi: 10.1109/TVT.2007.906878.

[14] Y. Liu, Y. Wang, and G. Chang, “Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm,” IEEE Trans. Intell. Transp. Syst., vol. 18, no. 1, pp. 2734–2743, Oct. 2017. Accessed: Jun. 5, 2020, doi: 10.1109/TITS.2017.2657649.

[15] C. Zhang, X. Lin, R. Lu, and P. H. Ho, “RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks,” in Proc. IEEE Int. Conf. Commun., Beijing, China, May 2008, pp. 1451–1456.

[16] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages, IEEE Standard 1609.2-2006, Jul. 2006.

[17] Security User Manual, ETSI Stack Softw., Cohda Wireless Pty Ltd., Wayville, SA, Australia, 2017.

[18] K.-A. Shim, “Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree,” IEEE Trans. Wireless Commun., vol. 12, no. 11, pp. 5386–5393, Nov. 2013. Accessed: Jun. 15, 2020, doi: 10.1109/TWC.2013.100313.120318.

[19] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” J. Comput. Secure., vol. 15, no. 1, pp. 39–68, Jan. 2007.

[20] H. Hassouny, A. E. Samhat, C. Bassil, and A. Laouiti, “Vanet security threats, challenges and solutions: A survey,” Veh. Commun., vol. 7, pp. 7–20, Jan. 2017. Accessed: May 25, 2020, doi: 10.1016/j.vehcom.2017.01.002.

[21] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, “Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks,” IEEE Access, vol. 6, pp. 2241–2250, Dec. 2018. Accessed: Jun. 15, 2020, doi: 10.1109/ACCESS.2017.2782672.

[22] Y.-N. Liu, S.-Z. Lv, M. Xie, Z.-B. Chen, and P. Wang, “Dynamic anonymous identity authentication (DAIA) scheme for VANET,” Int. J. Commun. Syst., vol. 32, no. 5, p. e3892, Mar. 2019. Accessed: May 25, 2020, doi: 10.1002/dac.3892.

[23] Z.-C. Liu, L. Xiong, T. Peng, D.-Y. Peng, and H.-B. Liang, “A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” IEEE Access, vol. 6, pp. 26307–26317, May 2018. Accessed: Jun. 16, 2020, doi: 10.1109/ACCESS.2018.2834224.

[24] S. Tangade, S. S. Manvi, and P. Lorenz, “Decentralized and scalable privacy-preserving authentication scheme in VANETs,” IEEE Trans. Veh. Technol., vol. 67, no. 9, pp. 8647–8655, Sep. 2018. Accessed: Jun. 16, 2020, doi: 10.1109/TVT.2018.2839979.

[25] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, “HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETS,” Veh. Commun., vol. 14, pp. 15–25, Oct. 2018. Accessed: May 25, 2020, doi: 10.1016/j.vehcom.2018.09.003.

[26] M. A. Alazawzi, H. Lu, A. A. Yassin, and K. Chen, “Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network,” IEEE Access, vol. 7, pp. 71424–71435, May 2019. Accessed: Jul. 3, 2020, doi: 10.1109/ACCESS.2019.2919973.

[27] S. O. Ogundoyin, “An efficient, secure and conditional privacy-preserving authentication scheme for vehicular ad-hoc networks,” J. Inf. Assurance Secur., vol. 11, pp. 179–192, Dec. 2017.

[28] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECP: Efficient conditional privacy preservation protocol for secure vehicular communications,” in Proc. 27th Conf. Comput. Commun. (INFOCOM), Apr. 2008, pp. 1903–1911.

[29] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, “An efficient identity-based batch verification scheme for vehicular sensor networks,” in Proc. IEEE INFOCOM, Apr. 2008, pp. 816–824, 2007.

[30] F. Eckermann, M. Kahler, and C. Wietfeld, “Performance analysis of C-V2X mode 4 communication introducing an open-source C-V2X simulator,” in Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall), Honolulu, HI, USA, Sep. 2019, pp. 1–5.

[31] I. Ali, A. Hassan, and F. Li, “Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey,” Veh. Commun., vol. 16, pp. 45–61, Apr. 2019. Accessed: May 25, 2020, doi: 10.1016/j.vehcom.2019.02.002.

[32] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, “2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET,” IEEE Trans. Veh. Technol., vol. 65, no. 2, pp. 896–911, Feb. 2016. Accessed: Jun. 15, 2020, doi: 10.1109/TVT.2015.2402166.

[33] P. Mundhe, V. K. Yadav, S. Verma, and S. Venkatesan, “Efficient lattice-based ring signature for message authentication in VANETs,” IEEE Syst. J., early access, Apr. 13, 2020. Accessed: Oct. 7, 2020, doi: 10.1109/JSYST.2020.2980207.

[34] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography. Berlin, Germany: Springer, 2009. Accessed: Feb. 4, 2020, doi: 10.1007/978-3-540-88702-7.

[35] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, “PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks,” IEEE Trans. Depend. Secur. Comput., early access, Mar. 11, 2019. Accessed: Oct. 5, 2020, doi: 10.1109/TDSC.2019.2904274.

[36] J. Cui, J. Zhang, H. Zhong, and Y. Xu, “SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter,” IEEE Trans. Veh. Technol., vol. 66, no. 11, pp. 10283–10295, Nov. 2017. Accessed: Oct. 5, 2020, doi: 10.1109/TVT.2017.2808207.

[37] V. Balasubramanian, S. Otoum, M. Aaloqiyi, I. Al Ridhawi, and Y. Jararweh, “Low-latency vehicular edge: A vehicular infrastructure model for 5G,” Simul. Model. Pract. Theory, vol. 98, Jan. 2020, Art. no. 101968. Accessed: Oct. 6, 2020, doi: 10.1016/j.simpat.2019.101968.

[38] M. M. Buyu Taha, S. Chaisiri, and R. K. L. Ko, “Trusted tamper-evident data provenance,” in Proc. IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, Aug. 2015, pp. 647–653.