A Novel Identity-Based Privacy-Preserving Anonymous Authentication Scheme for Vehicle-to-Vehicle Communication

Yasin Genc[1, *], Cagatay Korkuc[1], Nilay Aytas[2], Erkan Afacan[1], Murat H. Sazli[3], Erdem Yazgan[4]
[1]Department of Electrical-Electronics Engineering, Faculty of Engineering, Gazi University, 06570 Maltepe/Ankara, Turkey
[2]Department of Electrical-Electronics Engineering, Faculty of Engineering, Kirikkale University, 71450 Yahsihan/Kirikkale, Turkey
[3]Department of Electrical and Electronics Engineering, Faculty of Engineering, Ankara University, 06830 Golbasi/Ankara, Turkey
[4]Department of Electrical-Electronics Engineering, Faculty of Engineering, TED University, 06420 Cankaya/Ankara, Turkey
[*]yasin.genc@gazi.edu.tr, cagatay.korkuc1@gazi.edu.tr, nilayaytas@kku.edu.tr, e.afacan@gazi.edu.tr, sazli@eng.ankara.edu.tr, erdem.yazgan@tedu.edu.tr

***Abstract*—This paper proposes a novel bilinear pairing-free identity-based privacy-preserving anonymous authentication scheme for vehicle-to-vehicle (V2V) communication, called "NIBPA". Today, vehicular ad hoc networks (VANETs) offer important solutions for traffic safety and efficiency. However, VANETs are vulnerable to cyberattacks due to their use of wireless communication. Therefore, authentication schemes are used to solve security and privacy issues in VANETs. The NIBPA satisfies the security and privacy requirements and is robust to cyberattacks. It is also a pairing-free elliptic curve cryptography (ECC)-based lightweight authentication scheme. The bilinear pairing operation and the map-to-point hash function in cryptography have not been used because of their high computational costs. Moreover, it provides batch message verification to improve VANETs performance. The NIBPA is compared to existing schemes in terms of computational cost and communication cost. It is also a test for security in the random oracle model (ROM). As a result of security and performance analysis, NIBPA gives better results compared to existing schemes.**

***Index Terms*—Connected car; Elliptic curve cryptography; Identity-based; Vehicular ad hoc network; Communication.**

I. Introduction

Intelligent transportation systems (ITS) that increase traffic efficiency and provide traffic safety are important parts of smart cities. Communication from vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), such as vehicle-to-network (V2N) and vehicle-to-grid (V2G), has become widespread thanks to the development of 5G and beyond, and the internet of things (IoT) technologies. VANET is a vehicular network that enables vehicles to communicate with each other and with the infrastructure. It provides V2V and V2I communication using dedicated short range communications (DSRC) as per the IEEE 802.11p standard [1]. The design of this network is critical to security, privacy, and efficiency. Because if there is a lack of security and privacy, VANET can be cyberattacked. This cyberattack can lead to theft of personal data, traffic accidents, injuries, and even deaths [2]. For this reason, authentication schemes that protect privacy are used in the design of these networks for secure communication. The privacy-preserving authentication (PPA) scheme based on cryptographic methods is used to ensure privacy and security in VANETs and Internet of Vehicles (IoV) [3]–[13]. There are many cryptographic methods used in the PPA schemes such as paring-based cryptography, elliptic curve cryptography (ECC), certificateless cryptography, and RSA (Rivest-Shamir-Adleman). However, ECC has advantages over other public-key cryptography schemes. The proposed NIBPA scheme is based on ECC because it uses a very small key size compared to other schemes for the same level of security. Thus, it provides advantages in parameters such as computational cost, storage space, bandwidth, and power consumption [14]. There are three important criteria in the design of the PPA scheme in VANETs: anonymity of vehicle identities, security against cyberattacks, and low computational and communication costs. The reason for the anonymity of the vehicles is to prevent vehicle tracking. If the vehicle sending the message is detected by hackers, a serious security problem will occur in the VANET. However, if malicious behaviour of any vehicle is detected, the vehicle can only be removed from VANET by the central authority, so privacy is conditional [4], [5]. VANETs must have high performance to be used in practical traffic applications and be secure. For this, the computation and communication costs should be quite low.

A. Related Work

In the literature, many PPA schemes have been proposed

Manuscript received 23 March, 2022; accepted 7 April, 2023.
This research was supported by the TUBITAK 2211-E domestic doctoral scholarship programme.

to provide privacy and security and increase efficiency in VANETs or IoV [3]–[13], [15]–[18]. Raya and Hubaux [8] proposed an anonymous authentication scheme based on the public-key infrastructure (PKI). Key pairs and certificates are uploaded to the on-board unit (OBU) to create an anonymous identity. However, this requires high storage and is inefficient. Lu, Lin, Zhu, Ho, and Shen [9] proposed a new solution based on the temporary distribution of anonymous certificates to vehicles by road-side unit (RSU). But this scheme is inefficient because it requires temporary certificates for every vehicle in the broadcast domain of RSUs. In the PKI, vehicles use public-key, private-key, and certificates from the central authority for authorisation. Certificates are used for public-key distribution, which is one of the important issues of public-key cryptography methods. Certificate management incurs additional costs. Using user identity information as a public-key with identity-based cryptography offers a solution to this problem. The identity information of the users, IP address, MAC address, email address, phone number, IMEI number [19], and private, non-repudiation information that will identify them can be a public-key, such as vehicle chassis and licence plate numbers. Therefore, the identity-based scheme significantly decreases the communication cost and computational cost by eliminating the need for certification. Zhang, Lu, Lin, Ho, and Shen [10] proposed a PPA scheme that uses identity-based cryptography. In this scheme, neither the vehicle nor the RSU needs a certificate. Also, it can perform batch verification for many messages. However, this scheme is insecure against repudiation and replay attacks [16]. Ali and Li [17] and others [3], [11], [12], [18] also proposed an identity-based PPA scheme for VANETs. The PPA scheme has also been proposed in IoV [13]. These schemes use bilinear pairing operations and/or map-to-point hash functions. But these operations are very costly regarding computation processes. As a solution to this problem, He, Zeadally, Xu, and Huang [7] proposed the identity-based bilinear pairing-free PPA scheme using ECC. Similarly, in [4]–[6], ECC-based bilinear pairing-free schemes have been proposed. Xiong, Wang, Wang, Zhou, and Luo [4] proposed a conditional PPA scheme for VANETs, called "CPPA-D". This scheme provides double insurance for private keys. Li *et al*. [5] proposed an efficient and provably-secure PPA scheme. In this scheme, the message signing performance is quite good, but the message verification performance is low. Ali, Lawrence, and Li [20] proposed an identity-based signature scheme for V2V communication. It has high performance and is pairing-free. However, in [21], it was proved that this scheme is not secure. Alazzawi, Lu, Yassin, and Chen [22] proposed an authentication scheme for VANETs. This scheme does not support unlinkability. Cui, Zhang, Zhong, and Xu [15] proposed the ECC-based scheme (SPACF) using a cuckoo filter and binary search. They tried to increase the efficiency of batch verification. As a result, the motivation for this paper is to propose a high-performance PPA scheme for VANETs without sacrificing security.

B. Our Contributions

The contributions of the NIBPA scheme for V2V communication in VANET are as follows.

– NIBPA is a novel identity-based anonymous bilinear pairing-free PPA scheme using ECC. It can also perform batch verification.

– In addition, it is secure against adaptive selected messages in ROM and satisfies other security requirements.

– Finally, it is a lightweight scheme that provides high performance compared to existing schemes.

C. Organisation

The remainder of this paper is organised as follows. In Section II, ECC, bilinear pairing, VANETs, and security and privacy requirements are explained. In Section III, the proposed NIBPA scheme is designed. In Section IV, the implementation of the NIBPA scheme is carried out. In Section V, we perform a security analysis of the NIBPA. In Section VI, a performance analysis is realised and the computation cost and communication cost are compared with other existing schemes. Finally, in Section VII, results and future work are given.

II. Definitions and Background

In this section, ECC, bilinear pairing, VANETs, and security and privacy requirements are briefly introduced.

A. Elliptic Curve Cryptography (ECC)

ECC is a public-key cryptography method that uses two keys: the public-key and the private-key. The security of ECC is based on the difficulty of elliptic curve discrete logarithm problem (ECDLP). Mathematical operations in the ECC are performed on finite fields because they give more efficient and accurate results [23].

Let us define a non-singular elliptic curve $E(a,b)$ over a finite field $\mathbb{F}_p$ denoted as $E/\mathbb{F}_p$

$$E: y^2 = x^3 + ax + b \pmod{p}, \tag{1}$$

where p is a large prime number and $a,b \in \mathbb{F}_p$ constant integers less than p. a and b satisfy in (2)

$$4a^3 + 27b^2 \neq 0 \pmod{p}. \tag{2}$$

Suppose G is a cyclic additive group. The number of all points on $E(a,b)$ and infinity point (O) forms an additive elliptic curve group G with generator point P and of order q. There are three main mathematical operations used in ECC on points: point addition, point doubling, and scalar multiplication.

– Point addition: For two different points P and Q on the elliptic curve $E(a,b)$, over finite field $\mathbb{F}_p$, point addition can be calculated as $P+Q=R \in G$.

– Point doubling: For any point P on the elliptic curve $E(a,b)$, over finite field $\mathbb{F}_p$, point doubling can be calculated as $P+P=2P \in G$.

– Scalar multiplication: For any point P on the elliptic curve $E(a,b)$, over finite field $\mathbb{F}_p$, scalar multiplication

can be calculated as in (3), where $k \in Z_q^*$ and $P \in G$

$$kP = P + P + P + ... + P \ (k \ times). \tag{3}$$

– ECDLP: Suppose two different points P and Q of a group G on the elliptic curve $E(a,b)$. Finding the value of $k \in Z_q^*$ in (4) is quite difficult [23]

$$Q = k \cdot P. \tag{4}$$

B. Bilinear Pairing

Let us define a multiplicative group G_1 and an additive group G with the order q. $\tilde{e}: GxG \to G_1$ indicates a bilinear pairing which satisfies the following three situations.

– Bilinear: $\tilde{e}(xP, yQ) = \tilde{e}(P,Q)^{xy}$, where $x, y \in Z_q^*$ and $P, Q \in G$.

– Non-degenerate: $\tilde{e}(P,Q) \neq 1$, where $P, Q \in G$.

– Computable: $\tilde{e}(P,Q) \in G_1$ can be computed efficiently, where $P, Q \in G$ [24].

C. Vehicular Ad Hoc Networks (VANETs)

VANETs are used in ITS for many purposes such as connection between vehicles (V2V), connection of vehicles with infrastructure (V2I), safety, and optimisation in traffic. It consists of three basic units: RSU, OBU, and central authority (CA) [2], [25]. A basic VANET model is shown in Fig. 1. Let us explain the basic units of VANET below.

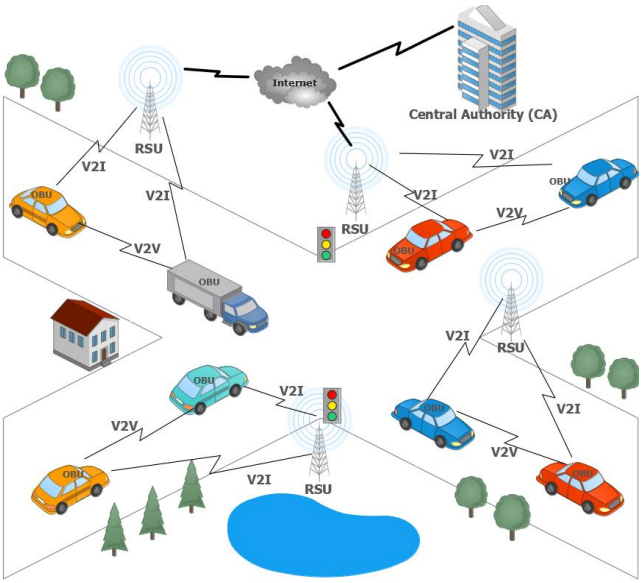

Fig. 1. Basic model of the vehicular ad hoc network (VANET).

1. *Road-Side Unit (RSU)*

RSUs are roadside wireless communication devices that provide communication between vehicles and the central unit. V2I communication is established between roadside units and vehicles [6]. RSUs send information to vehicles within communication ranges to provide better traffic safety and management [7]. It also collects routine information such as road condition, weather condition, direction of other vehicles with sensors and transmits this information to vehicles within range [5], [7], [17].

2. *On-Board Unit (OBU)*

An OBU is a tamper-proof device (TPD) that can perform cryptographic operations and store secret information [7]. Thanks to OBU, vehicles communicate with other vehicles (V2V) and roadside units (V2I) with the help of the DSRC protocol [12]. This device is the black box of the vehicle. OBUs regularly broadcast some useful information to other vehicles and RSUs, such as locations, directions, speeds, and traffic accidents [3].

3. *Central Authority (CA)*

CA is the centre of management for VANETs [11]. Vehicles and RSUs that want to be included in VANET are registered in the network structure by the CA [6], [12]. It gives them an anonymous identity and private key. The real identity of the vehicles is known only to the CA.

D. Security and Privacy Requirements

We define the security and privacy requirements for secure communication in VANETs.

1. *Message authentication and integrity*

When the vehicle or RSU receives a message, it checks the integrity of the message and the identity of the sender. The integrity of the message guarantees that no third parties have made changes to the message [17]. Identity check is used to determine whether it is sent by the vehicle or RSU in VANET [6].

2. *Non-repudiation*

A RSU and a vehicle cannot reject messages they have sent [4]. In this way, malicious messages can be detected and the sender can be determined.

3. *Identity privacy-preserving*

Vehicle identities must be anonymous. Any other vehicle, RSU and attackers should not be able to determine the real identities of other vehicles based on the messages sent.

4. *Traceability and revocability*

Even if the identities of the vehicles are to be covered, in some cases, such as fines or cancellation of identity, the real identity of the vehicles may be needed. The real identities of the vehicles can only be uncovered by the CA.

5. *Unlinkability*

Vehicles, RSU, and attackers should not be able to detect if two or more of the sent messages are from the same vehicle [16].

6. *Impersonation attack*

Vehicles, RSU, and attackers should not be able to legally create a signature on behalf of another vehicle.

7. *Man in the middle attack*

Vehicles, RSU, and attackers should not be able to manipulate messages between two vehicles.

III. The Proposed NIBPA Scheme

The proposed NIBPA scheme consists of four phases: system setup phase, anonymous identity generation and registration phase, message signing phase, and single and batch message verification phase. The flow chart of the proposed NIBPA scheme is shown in Fig. 2. The notation and descriptions used in the design of the NIBPA are shown in Table I. Let us examine in detail the four phases of the

NIBPA scheme that follow.

A. System Setup Phase

1. The CA selects a non-singular elliptic curve $E(a,b)$ over finite field $\mathbb{F}_p$. In the $y^2 = x^3 + ax + b \pmod p$, p is a very large prime number and $a,b \in \mathbb{F}_p$ constant integers less than p. The a and b values should satisfy the $4a^3 + 27b^2 \neq 0 \pmod p$. If the equation is not satisfied, the values of a and b are reselected. Later, a generation point P with order q is chosen for $E(a,b)$.

2. The CA selects two one-way hash functions, $H_1 : \{0,1\}^* \; x \; G \rightarrow Z_q^*$ and $H_2 : \{0,1\}^* \rightarrow Z_q^*$.

3. The CA selects a random private key $\delta \in Z_q^*$. δ is the private key known only to the CA. Later, it calculates public-key $P_{CA} = \delta \cdot P$.

4. The CA transmits the public parameters $\{E, p, q, P, P_{CA}, H_2\}$ to all vehicles. The one-way hash function H_1 is used to identify vehicles, so it is used only by the CA.

B. Anonymous Identity Generation and Register Phase

In this phase, the vehicles are registered by the CA. The registration of vehicles to the central unit (CU) is done using licence plates. Based on the licence plate number, which is the real identity of the vehicles, an anonymous identity is created and delivered to the vehicles. Let us examine these phases below.

1. The vehicle V_i applies to the CA for registration with ID_i plate number. The CA selects n numbers random private key $k_i^x \in Z_q^*$ for vehicles where $(x = 1...n)$. The i shows the registered vehicle number $(V_i, V_{i+1}, V_{i+2}...)$.

2. Anonymous identities (AID_i^x) are calculated by the CA using the licence plate numbers (ID_i) of the vehicles. The CA calculates public-keys of vehicle V_i with $P_i^x = k_i^x \cdot P_{CA}$. Later, anonymous identities calculation is given in (5)

$$AID_i^x = ID_i \oplus H_1(\delta \,\|\, P_i^x). \tag{5}$$

3. The parameters $\{P_i^x, AID_i^x, k_i^x\}_{x=1}^n$ are sent to the registered vehicle V_i via a secure channel and preloaded into the TPD for use in signature generation (n numbers). The number of n may vary according to the TPD capacity of the vehicle. The parameters are loaded into the TPD of the vehicle by performing this phase at certain intervals.

C. Message Signing Phase

Mathematical operations are performed on the TPD in vehicles. Messages are signed by performing the following steps before being sent to other vehicles.

1. The vehicle V_i selects a random private key $s_i \in Z_q^*$.

2. The vehicle V_i calculates $Q_i = s_i \cdot P_{CA}$.

3. The message is hashed using the vehicle's anonymous identity (AID_i^x), private key s_i, and timestamp (Ts_i). Then, λ_i^x is calculated using the one-way secure hash function H_2 according to (6)

$$\lambda_i^x = H_2(message_i \,\|\, AID_i^x \,\|\, Ts_i \,\|\, Q_i). \tag{6}$$

4. The vehicle V_i generates its digital signature σ_i^x as in (7). In this equation, λ_i^x is multiplied by the signature private key s_i and the result is summed with the vehicle's private key k_i^x

$$\sigma_i^x = k_i^x + \lambda_i^x \times s_i \pmod q. \tag{7}$$

5. Finally, the vehicle V_i that wants to send a message to the vehicles around it sends the parameters $\{\sigma_i^x, AID_i^x, P_i^x, Q_i, Ts_i\}$ along with the $message_i$.

D. Message Verification Phase

When the vehicle V_i receives a message from other vehicles, it is checked if the message is sent from a registered vehicle and whether the integrity of the message is satisfactory. The message verification phase is proved for single message and batch message.

1. First, the timestamp (Ts_i) is checked. If it is not within the specified time range ΔT, the message is rejected. Thus, messages that do not arrive on time are rejected before the message verification phase.

2. The vehicle V_j that receives the message checks whether it provides (8) using the parameters $\{\sigma_i^x, message_i, AID_i^x, P_i^x, Q_i, Ts_i\}$ sent with the single message. If not, the message is rejected

$$\sigma_i^x \cdot P_{CA} \stackrel{?}{=} P_i^x + \lambda_i^x \cdot Q_i. \tag{8}$$

Let us prove the correctness of (8)

$$\begin{aligned} \sigma_i^x \cdot P_{CA} &= (k_i^x + \lambda_i^x \times s_i) \cdot P_{CA} \\ &= k_i^x \cdot P_{CA} + H_2(message_i \,\|\, AID_i^x \,\|\, Ts_i \,\|\, Q_i) \times s_i \cdot P_{CA} \\ &= P_i^x + \lambda_i^x \cdot Q_i. \end{aligned} \tag{9}$$

Thus, single message verification has been proven.

When the vehicle receives multiple messages, it performs the verification of the messages very quickly thanks to batch verification.

3. If a batch message is sent to the vehicle, it is checked whether (10) is satisfied or not

$$(\sum_{i=1}^{n} \sigma_i) \cdot P_{CA} \stackrel{?}{=} \sum_{i=1}^{n} P_i + \sum_{i=1}^{n} Q_i. \tag{10}$$

Let us prove the correctness of (10)

$$(\sum_{i=1}^{n} \sigma_i^x) \cdot P_{CA} \stackrel{?}{=} (\sum_{i=1}^{n} k_i^x + \sum_{i=1}^{n} \lambda_i^x \times s_i) \cdot P_{CA},$$

$$(\sum_{i=1}^{n}\sigma_i^x)\cdot P_{CA} \stackrel{?}{=} \sum_{i=1}^{n}k_i^x\cdot P_{CA}+(\sum_{i=1}^{n}\lambda_i^x\times s_i)\cdot P_{CA},$$

$$(\sum_{i=1}^{n}\sigma_i^x)\cdot P_{CA}=\sum_{i=1}^{n}P_i^x+\sum_{i=1}^{n}\lambda_i^x\cdot Q_i. \quad (11)$$

Thus, batch message verification has been proven.

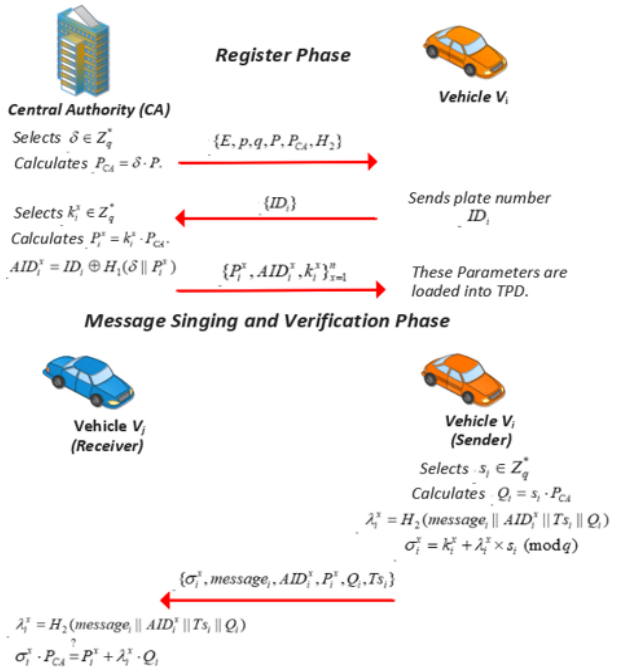

Fig. 2. The flow chart of the proposed NIBPA scheme.

TABLE I. NOTATIONS USED AND DESCRIPTION.

Symbol	Description
V_i, V_j	The i^{th} and j^{th} vehicle
ID_i	V_i's real identity, licence plate number
AID_i	Anonymous identity of vehicle V_i
E (a, b)	An elliptic curve
CA	Central authority
CU	Central unit
TPD	Tamper proof device
$Message_i$	Message sent by the vehicle V_i
σ_i	Signature of vehicle V_i
$H(.)$	One-way hash function
$\|$	Concatenation operator
$\oplus$	XOR operator
G	Additive cyclic group
G_1	Multiplicative group
q	Order of G and G_1
$\mathbb{F}_p$	Prime finite field
P	Generator point

IV. Implementation

In this section, the implementation of the message signing and message verification phase of the proposed NIBPA scheme is performed. In this process, the real-value NIST P-256 elliptic curve parameters and the SHA-256 hash function are used.

– Vehicle V_i computes λ_i^x using the following parameters:

AID_i^x = (99069487708869920880551879220652720035053029167298784326783672825474250044361);

$message_i$ = Attention there is an accident!!!!;

Ts_i = 21.09.2022, 10:55 PM;

s_i = 836215540579322464103324601912105606990208688788714280907824727273968887587 04;

P_{CA} = (40526504406281237348549802247570378033060992439814543468537628735201812047966,1073066635862397181402230257151710760684835811269666041203390738920228130844 43);

$Q_i = s_i \cdot P_{CA}$ = (85892232105674339761722327760417389894270340540266626951082514939652962505294,392114085037778460016418306073041723423719438289176938647578733607834204275 59);

$\lambda_i^x = H_2(message_i \| AID_i^x \| Ts_i \| Q_i)$ = (6766404341654892933053010161926029469471814875242721285847038977865656044737).

– Vehicle V_i computes the signature $\sigma_i^x = k_i^x + \lambda_i^x \times s_i$ using the following parameters:

k_i^x = 360355061284105310315944295036709406409644608050546485990533131555841408967 50;

$\sigma_i^x = k_i^x + \lambda_i^x \times s_i \pmod q$ =10333779608249543369095703995722412923120304445920175817443988927772448056 8545.

Thus, the signature is generated and sent to the receiving vehicle V_j along with other parameters $\{AID_i^x, P_i^x, Q_i, Ts_i\}$.

– The vehicle V_j receiving the message performs the verification of the message using the parameters. It computes $\lambda_i^x = H_2(message_i \| AID_i^x \| Ts_i \| Q_i)$ using the parameters sent by the vehicle V_i.

– Later, it checks whether the equality $\sigma_i^x \cdot P_{CA} \stackrel{?}{=} P_i^x + \lambda_i^x \cdot Q_i$ is satisfied. For this, it performs the following calculations and compares the results. If results are the same, the signature and message are valid.

$\sigma_i^x \cdot P_{CA}$ = (83495476239940053712207098841341712477425967119375665026730542678982493671 0,90708939564788021901350481705165407118885147285722342277819008468288706269050);

$P_i^x + \lambda_i^x \cdot Q_i$ = (83495476239940053712207098841341712477425967119375665026730542678982493671 0,90708939564788021901350481705165407118885147285722342277819008468288706269050).

Thus, equality is provided $\sigma_i^x \cdot P_{CA} = P_i^x + \lambda_i^x \cdot Q_i$, the signature and message are verified.

V. Security Analysis

In this section, the security analysis of the NIBPA scheme is performed. Firstly, we will analyse the security of it in the ROM. The following steps are performed to check the

security and privacy of NIBPA according to the security and privacy requirements explained in Section II.

A. Random Oracle Analysis

A game is set up to perform the security analysis of the NIBPA scheme and to measure the proficiency of the adversary against this scheme. This game is played between the challenger and the adversary *Adv*. If the adversary *Adv* wins this game, the authentication security of the NIBPA will be disabled.

Suppose that the NIBPA scheme is secure against the adaptive chosen message in the random oracle model. Let us prove this assumption in the following.

– *Setup-Oracle*: Firstly, challenger generates the private key $\delta \in Z_q^*$ and calculates $P_{CA} = \delta \cdot P$. Later, it sends all the parameters $\{E, p, q, P, P_{CA}, H_2\}$ to adversary *Adv*.

– *H₂-Oracle*: Challenger keeps a list in the format of a $(message_i, AID_i^x, Ts_i, Q_i, \lambda_i^x)$ for storing queries and answers. The list is denoted as *L*. Adversary *Adv* perform $(message_i, AID_i^x, Ts_i, Q_i)$ query. Challenger checks if the $(message_i, AID_i^x, Ts_i, s_i, \lambda_i^x)$ is in *L*. If found in the *L* list, challenger sends $\lambda_i^x = H_2(message_i \| AID_i^x \| Ts_i \| Q_i)$ to adversary *Adv*. Otherwise, generates a random hash value λ_i^x, adds $(message_i, AID_i^x, Ts_i, Q_i, \lambda_i^x)$ parameters to *L*, and sends to hash value λ_i^x to adversary *Adv*.

– *Sign-Oracle*: Adversary *Adv* performs a sign query for the signature of the message. The challenger selects random numbers $s_i, \sigma_i^x, \lambda_i^x \in Z_q^*$, $AID_i^x \in G$. Later, calculates $Q_i = s_i \cdot P_{CA}$ and $P_i^x = \sigma_i^x \cdot P_{CA} - \lambda_i^x \cdot Q_i$. Then, adds parameters $(message_i, AID_i^x, Ts_i, s_i, \lambda_i^x)$ to the list *L*. Finally, sends $\{\sigma_i^x, message_i, AID_i^x, P_i^x, Q_i, Ts_i\}$ to *Adv*.

Adversary *Adv* generates a message $\{\sigma_i^x, message_i, AID_i^x, P_i^x, Q_i, Ts_i\}$ and checks if (8) is satisfied. If not, then play over. As a result, the NIBPA is secure. But if the forgery lemma [26] is taken into account, the adversary *Adv* can generate a different valid message $\{\sigma_i^{x*}, message_i, AID_i^x, P_i^x, Q_i^*, Ts_i\}$. Thus, (12) is satisfied $(Q_i^* = s_i^* \cdot P_{CA})$

$$\sigma_i^{x*} \cdot P_{CA} = P_i^x + (\lambda_i^{x*} \times s_i^*) \cdot P_{CA} \ (\mathrm{mod}\, q). \tag{12}$$

If (8) and (12) are arranged as follows, (13) and (14) are obtained:

$$\begin{aligned}(\sigma_i^x - \sigma_i^{x*}) \cdot P_{CA} &= (P_i^x + (\lambda_i^x \times s_i) \cdot P_{CA}) - (P_i^x + (\lambda_i^{x*} \times s_i^*) \cdot P_{CA}) \\ &= (\lambda_i^x \times s_i) \cdot P_{CA} - (\lambda_i^{x*} \times s_i^*) \cdot P_{CA}, \end{aligned} \tag{13}$$

$$(\sigma_i^x - \sigma_i^{x*}) \cdot P_{CA} = Q_i - Q_i^* \ (\mathrm{mod}\, q). \tag{14}$$

Equation (14) is quite difficult to solve because of ECDLP $(Q = x \cdot P)$. Thus, the proposed NIBPA scheme proves to be robust against the adaptive chosen message in the ROM.

B. Message Authentication and Integrity

The authentication and integrity of the message is checked by the vehicle V_i. Using the parameters $\{\sigma_i^x, AID_i^x, P_i^x, Q_i, Ts_i\}$ sent with the received message, it is checked whether (8) is provided or not. If (8) is satisfied, the authentication of the message and the integrity of the message are ensured. Thus, the NIBPA provides message authentication and integrity.

C. Non-Repudiation

Even if their anonymous identity (AID_i^x) is used in messages broadcast by vehicles, vehicles cannot deny their identity. If any vehicle rejects the message it produces, its real identity (ID_i) is revealed by the CA calculation with the $ID_i = AID_i^x \oplus H_1(\delta \| P_i^x)$. Thus, the NIBPA provides non-repudiation.

D. Identity Privacy-Preserving

The real identities of the vehicles are anonymised by the CA calculation with the $AID_i^x = ID_i \oplus H_1(\delta \| P_i^x)$. Vehicles send messages with their anonymous identities; therefore, their real identities are not known to other vehicles. Since the vehicle cannot be identified, it is protected against malicious intentions. The real identity of the vehicles can only be revealed by the CA. Thus, the NIBPA provides identity privacy-preserving.

E. Traceability and Revocability

The use of anonymous identity by vehicles does not mean that they will not be tracked. The vehicles that send fake messages that will endanger the security are determined, and the authorisation to send messages is cancelled. The CA tracks suspicious vehicles and reveals their true identities. Thus, these vehicles are removed from VANET, which prevents it from transmitting messages. The vehicle anonymous identity, $AID_i^x = ID_i \oplus H_1(\delta \| P_i^x)$, is calculated using the CA private key δ and the vehicle public-key P_i^x. The real identity of the vehicle V_i is revealed by calculating $ID_i = AID_i^x \oplus H_1(\delta \| P_i^x)$. Thus, the NIBPA provides traceability and revocability.

F. Unlinkability

V_i sends parameters $\{\sigma_i^x, message_i, AID_i^x, P_i^x, Q_i, Ts_i\}$ to other vehicles along with the message. The anonymous identity used by the vehicle changes with each message. The parameters $\{P_i^x, AID_i^x, k_i^x\}_{x=1}^n$ are sent to the registered vehicle V_i via a secure channel and preloaded into the TPD for use in signature generation. The digital signature and anonymous identity are different from each other in each message. Thus, the attacker cannot link the signature and the anonymous identity-based on messages.

G. Impersonation Attack

An attacker would need to create parameters

$\{\sigma_i^x, AID_i^x, P_i^x, Q_i, Ts_i\}$ for a vehicle to impersonate. However, since k_i and s_i are the private keys of the vehicle V_i, the attacker cannot do it. Thus, the NIBPA scheme is robust to impersonation attack.

H. Man in the Middle Attack

Since communication between vehicles is based on ID_i authentication, an attacker who is not registered with the CU cannot perform a man-in-the-middle attack.

VI. Performance Analysis

In this section, we analyse the performance of the NIBPA scheme in terms of computational cost and communication cost. We compare NIBPA with other schemes in [3]–[7] for performance analysis. NIBPA and the schemes in [4]–[7] are based on ECC and the scheme presented in [3] is based on bilinear pairing.

A. Computation Cost Analysis

The execution times and definitions of cryptographic operations used to determine the computational costs of the NIBPA scheme and other schemes are shown in Table II (ms: millisecond).

TABLE II. EXECUTION TIME OF CRYPTOGRAPHIC OPERATIONS.

Operation	Execution Time (ms)	Definition
T_{bp}	4.5726	Bilinear pairing operation
$T_{sm\text{-}bp}$	1.1906	Scalar multiplication on bilinear pairing
$T_{pa\text{-}bp}$	0.0039	Point addition on bilinear pairing
$T_{sm\text{-}ecc}$	0.3702	Scalar multiplication on ECC
$T_{ssm\text{-}ecc}$	0.0151	Small scalar multiplication operation on ECC ([1, 2^s], for s = 5)
$T_{pa\text{-}ecc}$	0.0023	Point addition on ECC
T_{mtp}	3.0158	Map-to-point hash function
T_h	0.0002	One-way hash function

The execution times of the concatenate and XOR operations used in computation are quite low, so these operators can be negligible in the computation cost analysis. For these calculations, computer platform running on Linux operating system with Intel (R) Core (TM) i7-7500U CPU processor and 8 GB RAM, PBC, and GMP cryptographic libraries in C++ programming language are used. The PBC and GMP cryptographic libraries are used together for pairing operations. The execution of each operation is repeated 100 times and the average value of the execution time of cryptographic operations is computed.

MS, OMV, and BMV denote message signing, single message verification, and batch message verification, respectively. In the scheme of Bayat, Barmshoory, Rahimi, and Aref in [3], the computational cost of MS consists of five scalar multiplications in bilinear pairing, one point addition in bilinear pairing, one map-to-point hash function, and two one-way hash functions. Thus, the execution time of MS is $5T_{sm\text{-}bp} + T_{pa\text{-}bp} + T_{mtp} + 2T_h$ = 8.9731 ms. The computational cost of OMV consists of three bilinear pairing operations: one-scalar multiplication on bilinear pairing, one map-to-point hash function, and one one-way hash function. Thus, the execution time of OMV is $3T_{bp} + T_{sm\text{-}bp} + T_{mtp} + T_h$ = 17.9244 ms. The computational cost of BMV consists of three bilinear pairing operations: (n) scalar multiplication in bilinear pairing, (3n - 3) point addition in bilinear pairing, (n) map-to-point hash function, and (n) one-way hash function. Thus, the execution time of the BMV is $3T_{bp} + (n)T_{sm\text{-}bp} + (3n - 3)T_{pa\text{-}bp} + (n)T_{mtp} + (n)T_h$ = 4.2183n + 13.7061 ms. In the same way, the execution times of MS, OMV, and BMV in [4]–[7] are computed. Finally, in the proposed NIBPA scheme, the computational cost of MS consists of one-scalar multiplication and one-way secure hash functions. Therefore, the execution time of MS is $T_{sm\text{-}ecc} + T_h$ = 0.3704 ms. The cost of OMV computation consists of two-scalar multiplication, one point addition, and a one-way hash function. Therefore, the execution time of OMV is $2T_{sm\text{-}ecc} + T_{pa\text{-}ecc} + T_h$ = 0.7429 ms. The computation cost of BMV consists of (n + 1) scalar multiplication, (2n - 1) point addition, and (n) one-way hash functions. Thus, the execution time of BMV is $(n + 1)T_{sm\text{-}ecc} + (2n - 1)T_{pa\text{-}ecc} + (n)T_h$ = 0.375n + 0.3679 ms. The comparison of the calculation costs analysis of the proposed NIBPA scheme and the other five schemes is shown in Table III. In Fig. 3, the computation costs of the NIBPA scheme and other schemes in MS and OMV are compared.

TABLE III. COMPARISON OF THE COMPUTATION COST ANALYSIS.

Scheme	MS (ms)	OMV (ms)	BMV (ms)
Bayat, Barmshoory, Rahimi, and Aref [3]	$5T_{sm\text{-}bp} + T_{pa\text{-}bp} + T_{mtp} + 2T_h$ = 8.9731	$3T_{bp} + T_{sm\text{-}bp} + T_{mtp} + T_h$ = 17.9244	$3T_{bp} + (n)T_{sm\text{-}bp} + (3n - 3)T_{pa\text{-}bp} + (n)T_{mtp} + (n)T_h$ = 4.2183n + 13.7061
Xiong, Wang, Wang, Zhou, and Luo [4]	$2T_{sm\text{-}ecc} + 2T_h$ = 0.7408	$3T_{sm\text{-}ecc} + T_{ssm\text{-}ecc} + 2T_{pa\text{-}ecc} + 2T_h$ = 1.1307	$(n + 2)T_{sm\text{-}ecc} + (n)T_{ssm\text{-}ecc} + (3n - 1)T_{pa\text{-}ecc} + (2n)T_h$ = 0.3926n + 0.7381
Li *et al*. [5]	$T_{sm\text{-}ecc} + 2T_h$ = 0.3706	$4T_{sm\text{-}ecc} + T_{pa\text{-}ecc} + 2T_h$ = 1.4835	$(2n + 2)T_{sm\text{-}ecc} + (n)T_{pa\text{-}ecc} + (2n)T_h$ = 0.7431n + 0.7404
Yao, Wang, Gan, Lin, and Huang [6]	$T_{sm\text{-}ecc} + T_h$ = 0.3704	$3T_{sm\text{-}ecc} + 2T_{pa\text{-}ecc} + 2T_h$ = 1.1156	$(2n + 1)T_{sm\text{-}ecc} + (3n - 1)T_{pa\text{-}ecc} + (2n)T_h$ = 0.7477n + 0.3679
He, Zeadally, Xu, and Huang [7]	$3T_{sm\text{-}ecc} + 3T_h$ = 1.1112	$3T_{sm\text{-}ecc} + 2T_{pa\text{-}ecc} + 2T_h$ = 1.1156	$(n + 2)T_{sm\text{-}ecc} + (2n)T_{ssm\text{-}ecc} + (3n - 1)T_{pa\text{-}ecc} + (2n)T_h$ = 0.4077n + 0.7381
Proposed Scheme: NIBPA	$T_{sm\text{-}ecc} + T_h$ = 0.3704	$2T_{sm\text{-}ecc} + T_{pa\text{-}ecc} + T_h$ = 0.7429	$(n + 1)T_{sm\text{-}ecc} + (2n - 1)T_{pa\text{-}ecc} + (n)T_h$ = 0.375n + 0.3679

The proposed NIBPA scheme provides 95.87 %, 50 %, 0.054 %, 0 %, and 66.67 % less execution time in MS compared to the schemes in [3]–[7], respectively. If we do the same comparison for OMV, it provides 95.86 %, 34.30 %, 49.92 %, 33.41 %, and 33.41 % less execution time than the schemes in [3]–[7], respectively. The improvement calculation as percentage for the scheme in [3]

is done with like $\frac{8.9731-0.3704}{8.9731}\times 100 = 95.87\,\%$.

The execution times of BMV for different message numbers (n = 5, n = 25, n = 50, n = 75, n = 100, n = 150, respectively) are compared in Fig. 4.

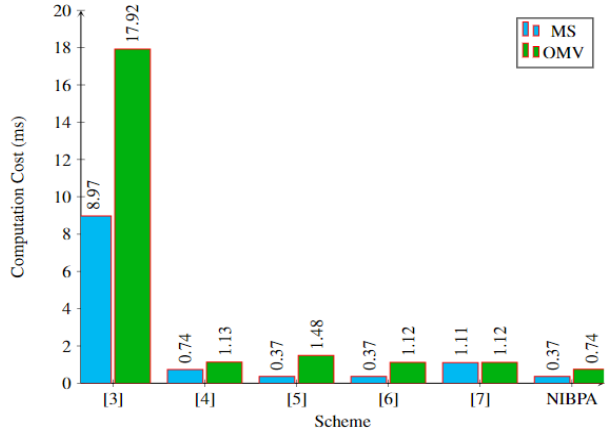

Fig. 3. Computation costs of MS and OMV.

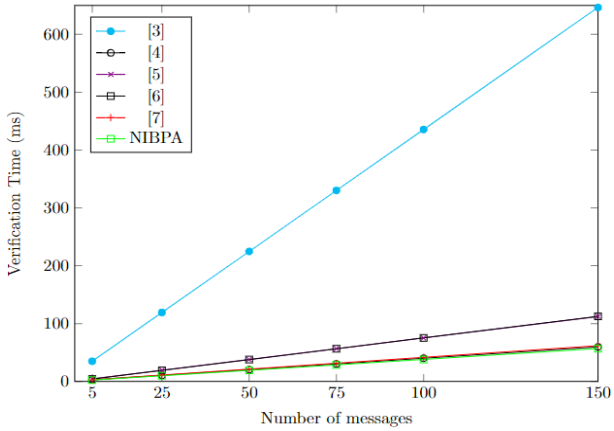

Fig. 4. Execution time of batch message verification.

The proposed NIBPA scheme performs batch message verification in less time than other schemes. It gives better results as the number of messages increases.

B. *Communication Cost Analysis*

Let us compare the communication cost of the NIBPA with the other five schemes. In computing the communication cost, let us assume the size of the elements in Z_q^*, the one-way hash function as 20 bytes and the size of the timestamp Ts_i as 4 bytes. At the same time, let us assume that the sizes of the elements in the multiplicative group G_1 and the addition cycle group G are 128 and 40 bytes, respectively. In the scheme in [3], the total communication cost of the $\{ID_1^i, ID_2^i, \sigma_i\} \in G_1$ and timestamp $\{T_i\}$ parameters sent by the vehicle is 128 × 3 + 4 = 388 bytes. In the same way, the total communication cost is computed in the schemes in [4]–[7]. Finally, in the proposed NIBPA scheme, the total communication cost of the parameters $\{AID_i^x, \sigma_i^x\} \in Z_q^*$, $\{P_i^x, Q_i\} \in G$, and timestamp $\{T_{Si}\}$ sent by the vehicle is 20 × 2 + 40 × 2 + 4 = 124 bytes. The comparison of the communication cost analysis of the NIBPA and the other five schemes is shown in Table IV.

TABLE IV. COMPARISION OF THE COMMUNICATION COST ANALYSIS.

Scheme	One message size (bytes)	Batch n messages size (bytes)
Bayat, Barmshoory, Rahimi, and Aref [3]	388	388n
Xiong, Wang, Wang, Zhou, and Luo [4]	128	128n
Li *et al.* [5]	144	144n
Yao, Wang, Gan, Lin, and Huang [6]	168	168n
He, Zeadally, Xu, and Huang [7]	144	144n
Proposed Scheme: NIBPA	124	124n

As seen in Table IV, the communication cost of the NIBPA is lower than the schemes in [3]–[7].

VII. Conclusions

In this paper, a novel identity-based privacy-preserving anonymous authentication scheme with ECC called "NIBPA" is proposed. It is used for V2V communication in VANETs. The proposed NIBPA scheme provides low computation cost and communication cost thanks to its pairing-free nature.

It can also perform batch message verification. Thus, it is a lightweight scheme that confirms a large number of messages faster. As a result of security analysis, it has been proven to satisfy privacy and security requirements. It has also proven to be a more cost-effective scheme compared to other existing schemes in terms of computation and communication costs. Message verification time is improved by 33.41 % to 95.86 % compared to existing schemes. Thus, the proposed NIBPA scheme is suitable for V2V communication in VANETs as it is efficient and secure. In future work, we are considering designing vehicle-to-everything (V2X) communication for 5G-enabled vehicular networks. We also plan to use technologies such as homomorphic encryption and blockchain in VANETs.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks", *IEEE Network*, vol. 34, no. 2, pp. 37–45, 2020. DOI: 10.1109/MNET.001.1900220.

[2] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, "A systematic review on security issues in vehicular ad hoc network", *Security and Privacy*, vol. 1, no. 5, p. e39, 2018. DOI: 10.1002/spy2.39.

[3] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification", *Wireless Net.*, vol. 21, pp. 1733–1743, 2015. DOI: 10.1007/s11276-014-0881-0.

[4] W. Xiong, R. Wang, Y. Wang, F. Zhou, and X. Luo, "CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs", *IEEE Trans. on Veh. Tech.*, vol. 70, no. 4, pp. 3456–3468, 2021. DOI: 10.1109/TVT.2021.3064337.

[5] J. Li *et al.*, "EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for

vehicular ad hoc networks", *Vehicular Communications*, vol. 13, pp. 104–113, 2018. DOI: 10.1016/j.vehcom.2018.07.001.

[6] M. Yao, X. Wang, Q. Gan, Y. Lin, and C. Huang, "An improved and privacy-preserving mutual authentication scheme with forward secrecy in VANETs", *Security and Communication Networks*, vol. 2021, art. ID 6698099, 2021. DOI: 10.1155/2021/6698099.

[7] 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. on Inf. Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015. DOI: 10.1109/TIFS.2015.2473820.

[8] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks", *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007. DOI: 10.3233/JCS-2007-15103.

[9] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications", in *Proc. of IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008, pp. 1229–1237. DOI: 10.1109/INFOCOM.2008.179.

[10] 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. of IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008, pp. 246–250. DOI: 10.1109/INFOCOM.2008.58.

[11] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs", *Comp. Comm.*, vol. 112, pp. 154–164, 2017. DOI: 10.1016/j.comcom.2017.09.005.

[12] J. Zhang, Q. Zhang, X. Lu, and Y. Gan, "A novel privacy-preserving authentication protocol using bilinear pairings for the VANET environment", *Wireless Communications and Mobile Computing*, vol. 2021, art. ID 6692568, 2021. DOI: 10.1155/2021/6692568.

[13] Y. Genc, N. Aytas, A. Akkoc, E. Afacan, and E. Yazgan, "ELCPAS: A new efficient lightweight certificateless conditional privacy preserving authentication scheme for IoV", *Vehicular Communications*, vol. 39, art. 100549, 2023. DOI: 10.1016/j.vehcom.2022.100549.

[14] Y. Genç and E. Afacan, "Implementation of new message encryption using elliptic curve cryptography over finite fields", in *Proc. of 2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, 2021, pp. 1–6. DOI: 10.1109/ICOTEN52080.2021.9493519.

[15] 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. 10283–10295, 2017. DOI: 10.1109/TVT.2017.2718101.

[16] S. Tangade, S. S. Manvi, and P. Lorenz, "Trust management scheme based on hybrid cryptography for secure communications in VANETs", *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5232–5243, 2020. DOI: 10.1109/TVT.2020.2981127.

[17] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs", *Vehicular Communications*, vol. 22, art. 100228, 2020. DOI: 10.1016/j.vehcom.2019.100228.

[18] B. Samra and S. Fouzi, "New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET", *Vehicular Communications*, vol. 34, art. 100414, 2022. DOI: 10.1016/j.vehcom.2021.100414.

[19] Y. Genç and E. Afacan, "Identity-based encryption in the Internet of Things", in *Proc. of 2021 29th Signal Processing and Comm. Applications Conf. (SIU)*, 2021, pp. 1–4. DOI: 10.1109/SIU53274.2021.9477945.

[20] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs", *Journal of Systems Architecture*, vol. 103, art. 101692, 2020. DOI: 10.1016/j.sysarc.2019.101692.

[21] Y. Song, C. Xu, Y. Zhang, and F. Li, "Comments on an identity-based signature scheme for VANETs", *Journal of Systems Architecture*, vol. 112, art. 101851, 2021. DOI: 10.1016/j.sysarc.2020.101851.

[22] M. A. Alazzawi, 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, 2019. DOI: 10.1109/ACCESS.2019.2919973.

[23] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2006. DOI: 10.1007/b97644.

[24] D. C. Dogan and H. Altindis, "Storage and communication security in cloud computing using a homomorphic encryption scheme based Weil pairing", *Elektronika ir Elektrotechnika*, vol. 26, no. 1, pp. 78–83, 2020. DOI: 10.5755/j01.eie.26.1.25312.

[25] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey", *Vehicular Comm.*, vol. 7, pp. 7–20, 2017. DOI: 10.1016/j.vehcom.2017.01.002.

[26] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures", *Journal of Cryptology*, vol. 13, pp. 361–396, 2000. DOI: 10.1007/s001450010003.