Hindawi
Complexity
Volume 2022, Article ID 8406649, 8 pages
https://doi.org/10.1155/2022/8406649

WILEY | Hindawi

Research Article

Cost-Efficient Privacy-Preserving Authentication and Key Management Scheme for Internet of Vehicle Ecosystem

Tahir Ali Shah,[1] Fahad Algarni,[2] Insaf Ullah,[3] Ako Muhammad Abdullah,[4,5] Fazal Noor,[6] and Muhammad Asghar Khan[3]

[1]*School of Computer, Jiangsu University of Science and Technology, Zhenjiang, Jiangsu Province, China*
[2]*College of Computing and Information Technology, The University of Bisha, Bisha, Saudi Arabia*
[3]*Hamdard Institute of Engineering & Technology, Hamdard University, Islamabad 44000, Pakistan*
[4]*University of Sulaimani, College of Basic Education, Computer Science Department, Sulaimaniyah, Kurdistan Region, Iraq*
[5]*Department of Information Technology, University College of Goizha, Sulaimaniyah, Kurdistan Region, Iraq*
[6]*Department of Computer and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia*

Correspondence should be addressed to Insaf Ullah; insafktk@gmail.com

Received 8 March 2022; Revised 21 April 2022; Accepted 25 April 2022; Published 3 June 2022

Academic Editor: Jawad Ahmad

Internet of vehicles (IoV) is an emerging area of advanced transportation systems, in which the functionality of traditional vehicular ad hoc networks (VANET) combined with the Internet of things (IoT). This technology allows vehicle users and drivers to interact in real time from anywhere and anytime. However, until recently, the major two problems that authentication and key management methods may solve are security and privacy. In this study, we offer a privacy-preserving authentication and key management scheme for the IoV environment that is computationally and communication cost-effective. We conducted a thorough security analysis, demonstrating that the proposed scheme is resistant to a variety of cryptographic attacks. We have included a cost analysis that indicates the proposed scheme is more efficient than IoV's current privacy-preserving authentication and key management schemes.

1. Introduction

Vehicular ad hoc network (VANET) has emerged as one of the most significant research fields in recent years, encompassing things such as vehicles, which include On-Board Units (OBU), Road-Side Units (RSU), and Trusted Authority (TA). An OBU is an electromagnetic device that is usually installed on a vehicle and used to send and receive data to and from the RSU [1]. It is made up of a resource command processor and resources, which store and restore data using a read/write memory [2]. RSUs are permanent communication gateways that feature an antenna, CPU, and read/write memory to enable wireless communication employing IEEE 802.11p radio technology between OBU and servers or the Internet [3]. The TA provides numerous premium Internet services to VANET subscribers through RSU, as well as protecting the entire vehicular network [4]. The Internet of things (IoT) allows smart connected objects to communicate with one another, expanding existing vehicular ad hoc networks (VANETs) into the Internet of vehicles (IoV) as a result of recent advancements in communication network technology [5].

The most essential services in IoV are traffic efficiency and road safety, which share real-time data through the Internet to reduce road accidents [6]. Figure 1 shows the usual flow diagram for IoV, which shows the communication process between entities such as the TA, OBU, and RSU.

Apart from standard IoV communication, the Fifth Generation (5G) cellular network is a viable choice for effectively delivering all of these services. The basic infrastructure for constructing a smart IoV environment will be provided by 5G, which will push vehicle network performance and capabilities needs to an acceptable level [7].

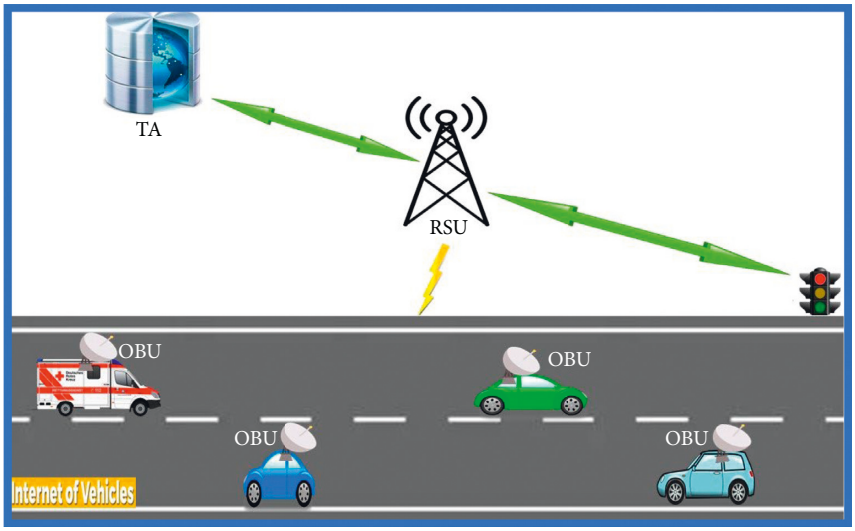

Figure 1: Basic flow of IoV.

Because the IoT is an open network, there are certain serious security risks that must be addressed. Indeed, users are growing increasingly concerned about the impact of modern technology on their privacy. For example, an attacker eavesdropping in on communications may exploit private information to trace down a specific vehicle and its driver's movements [8]. These malicious activities could jeopardize users' privacy as well as lead to robbery and physical injury [9]. Authentication and key agreement will be the most effective techniques for dealing with such attacks. Authentication is the process through which two or more participants in an IoV environment learn about each other before exchanging data [10]. Furthermore, before communicating with one another, the key management system allows all participants (e.g., OBU, RSU, and TA) to validate the messages by matching the generated keys [11].

Batch verifications [12] are a technique that, in addition to the two procedures mentioned above, provides for the authentication of numerous messages at once. The elliptic-curve cryptography (ECC) and Rivest Shamir Adleman (RSA) algorithms, which are well-known public-key methods and provide the same functions, are used in the majority of existing schemes, but the computation cost is still very high because key creation, signing, and decryption are all extremely slow, making them a little more difficult to implement securely.

To address the limitations of existing vehicle communication methods, this study uses hyperelliptic curve cryptography (HECC) to show a 5G vehicular network that is both safe and efficient while also lowering computational costs. As a result of the preceding debate, we have made the following contributions to this work:

(1) We propose an authentication and key management scheme with the help of HECC

(2) We conducted a thorough security study, which revealed that the proposed scheme is resistant to a variety of cyber-attacks

(3) We performed a computational cost study, comparing our proposed scheme to previously published approaches, and the findings demonstrate that the proposed scheme is more efficient.

1.1. Preliminaries. This section gives a short overview of the hyperelliptic curve idea and formal definition.

1.1.1. Hyperelliptic-Curve Cryptography. Hyperelliptic-curve cryptography was first developed by Miller and Koblitz, in 1988, which is the extent of an elliptic curve that depends on discrete logarithm problem in the Jacobian with genus two. Equation (1) represents the popular form of hyperelliptic curve of genus two on Jacobian group with finite field $\mathfrak{F}_q$:

$$B\colon a^2 + h(b)a = k(b)\mathrm{mod}q, \tag{1}$$

where $h(b) \in \mathfrak{F}[b]$ is a polynomial and degree $h(b) \le g$ and $k(b) \in \mathfrak{F}[b]$ is a monic polynomial and degree of $k(b) \le 2g + 1$.

1.1.2. Divisor. The finite formal sum of points on hyperelliptic curve is called divisor and represented in MumFord form as

$$R = (m(b), n(b)) = \left(\sum_{i=0}^{g} m_i b^i, \sum_{i=0}^{g-1} n_i b^i\right). \tag{2}$$

1.1.3. Jacobian Group. The divisors form an Abelian group which is called Jacobian group $J_c(\mathfrak{F}_q)$ and the order of the Jacobian group $o(J_c(\mathfrak{F}_q))$ is defined as

$$\left|(\sqrt{q} - 1)^{2g}\right| \le o\left(J_c\left(\mathfrak{F}_q\right)\right) \le \left|(\sqrt{q} + 1)^{2g}\right|. \tag{3}$$

1.1.4. Hyperelliptic-Curve Discrete Logarithm Problem (HECDLP). Let $Đ$ be divisor of order n in the Jacobian group $J_c(\mathfrak{F}_q)$; find an integer $b \in \mathfrak{F}_q$, such that

$$Đ_1 = b.Đ. \tag{4}$$

2. Related Work

Any entity in the IoV that receives relevant traffic messages must go through an authentication process to guarantee that the message's source is trustworthy and that the content is complete and legitimate. Many researchers have made contributions to the field of IoV network authentication methods in this regard. To assure vehicle legitimacy, Lu et al. [13] proposed a cost-effective conditional privacy-preserving (ECPP) authentication mechanism based on certificates. A vehicle can connect to other cars in the transmission range using its certificate in this scheme; however, if the certificate's time slot expires, the vehicle must visit an RSU to produce a new certificate. Zhang et al. [14] developed an identity-based batch verification (IBV) system, in which each vehicle stores crucial parameters and generates pseudonyms, allowing numerous messages to be evaluated at the same time using bilinear pairing characteristics.

Jiang et al. [15] used similar strategies to create an effective unidentified batch authentication methodology (ABAH) for effectively authenticating a large number of communications. Wang et al. [16] proposed a two-factor lightweight privacy-preserving authentication system (2FLIP), in which each On-Board Unit (OBU) is equipped with a perfect tamper-proof device (TPD) that stores a system key and generates a message authentication code (MAC) using the system key while signing a message. Each TPD's retention of the system key might result in a single point of failure. In DAPPA, each authorized vehicle gets two-member secrets from RSUs, and Zhang et al. [17] introduced a distributed aggregate privacy-preserving authentication approach (DAPPA) that can conduct batch verification without needing the use of an optimum TPD. Although their multiplications are the identical, these two-member secrets differ based on the vehicle. The discovered member secrets and the one-time identity-based aggregate signature may then be used by cars to do batch verification. However, because this DAPPA system includes several pairing operations, there is a significant verification delay when a large number of messages need to be validated.

Based on a registration list, Zhong et al. [18] developed a privacy-preserving conditional authentication approach (CPPARL). The proposed CPPARL allows RSU to collect and validate all messages sent by cars within its transmission range, after which it encrypts and sends out two bloom filters, one positive and one negative, using its secret key.

To mitigate failure of service (DoS) attacks, Liu et al. [19] proposed a puzzle-based pseudonymous authentication mechanism for a 5G vehicular network. In this scheme, each vehicle must solve a hash problem before transmitting a message. However, because messages are not sent at the proper moment, this approach has a significant communication cost. To achieve efficient message authentication, Huang et al. [3] suggested a safe and efficient privacy-preserving authentication strategy for automotive networks, which uses a registration list and elliptic-curve public-key cryptography. This solution, however, does not define the service profile identifier (SPID) validation time or the hash list update rate in order to enhance network performance.

Raja et al. [20] developed an RSU-based group authentication (RGA) system in which each vehicle in its range is assigned a group ID and group key pair, ensuring more secure communication while reducing network overhead. However, their technique has a high total computing cost. Hashem Eiza et al. [21] established secure video reporting services for 5G car networks, in which vehicles may quickly report a road accident by simply sending recorded video footage, while the reporter's identity and video data are kept private. However, because this technology is built for video transmission services, it is incompatible with other safety-related apps. Bouchelaghem and Omar [22] proposed a privacy-preserving pseudonym shifting technique for VANET; as a result, this scheme has certain security difficulties for OBU and traffic monitoring cameras-based tracking. Yao et al. [23] developed an enhanced mutual authentication strategy for VANETs that uses the ECC to provide forward secrecy; however, their proposed system has a significant computational cost and communication overhead owing to the usage of the elliptic curve.

3. Network Model

Figure 2 depicts our proposed IoV network system architecture, which includes three communication system partners: OBU, Trusted Authority (TA), and RSU, in that order. We used the substeps below to explain the function of each entity.

(1) OBU: it encrypts his identity and uses TA's public key to do a hash function. The hash values and the encrypted identifying text are subsequently transferred to TA. TA decrypts the encrypted text and applies the hash function to the decrypted text after receiving the encrypted text and hash value. It also analyses both hash values and, if they match, generates the public and private key for OBU and sends it via a secure channel. It produces the digital signature, secret key, and ciphertext of its identification and sends the authentication message to RSU after receiving the public and private key.

(2) TA: upon reception of encrypted text and hash value from OBU or RSU, TA first decrypts the encrypted text before applying the hash function to it. Furthermore, it compares both hash values and, if they match, generates the public and private key for OBU or RSU and delivered it via a secure route.

(3) RSU: it performs two execution processes on its identification, one of which is encryption using TA's public key and the other of which is a hash function. Then, it sends the encrypted text of identity along

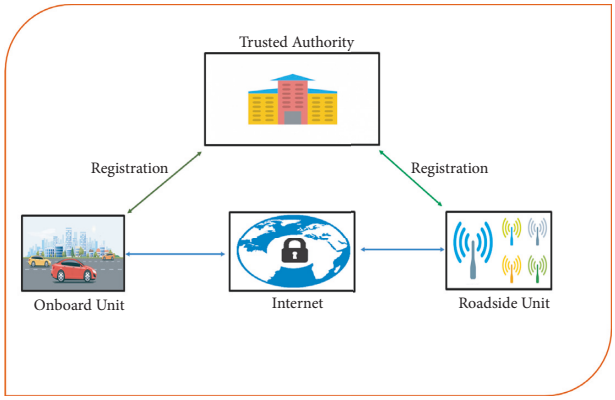

Figure 2: Network model for our proposed scheme.

with the hash values to TA. Upon reception of encrypted text and hash value, TA first decrypts the encrypted text and performs the hash function on the decrypted text. Furthermore, it compares both the hash values and, if it is matched, then produces the public and private key for OBU and dispatched it through a secure channel. When it is received, the public key and private key, further, received the authentication message from OBU, it performs the decryption process for cipher text and verification process for signature; if both the processes are performed successfully, then it set the secret key for further communications.

4. Proposed Mutual Authentication Scheme for IoV

Table 1 includes the symbols used in this scheme and the inclusive stages of our mutual authentication scheme for IoV explained as follows:

(i) Setup: here, the trusted authority (TA) computes $\chi = Đ.\mathscr{D}$ and sets χ as his public key and $Đ$ as his master private key, where $Đ$ has been choose randomly. Furthermore, it makes and publishes $\mathscr{F} = \{\chi, \text{HEC}, \mathscr{D}, F^Q, H\}$ as a global parameter set, where χ denotes the master public key of TA, HEC denotes a genus 2 hyperelliptic curve, $\mathscr{D}$ denotes a 80 bits devisor, F^Q denotes an order Q finite field and its value will be equal to 80 bits, and H represents a collision resistant and irreversible hash function.

(ii) Registrations: each Actor (A_i) with ID_{Ai} computes $\text{CID}_{Ai} = E_\chi(\text{ID}_{Ai})$ and $\text{HID}_{Ai} = H(\text{ID}_{Ai})$, where χ is the public key of TA and E_χ represent the encryption function that encrypts the value through the public key of TA. Then, A_i send $(\text{CID}_{Ai}, \text{HID}_{Ai})$ to TA. So, upon reception of $(\text{CID}_{Ai}, \text{HID}_{Ai})$, CA can compute $\text{ID}_{Ai} = D_Đ(\text{CID}_{Ai})$ and $\text{HID}_{Ai}/ = H(\text{ID}_{Ai})$, where $Đ$ is the private key of CA and $D_Đ$ represent the decryption function that decrypts the value through the private key of TA. Furthermore, CA compare $\text{HID}_{Ai}/ = \text{HID}_{Ai}$; if it is equal, then it computes $\ell_{Ai} = \beta_{Ai}.\mathscr{D}$, $\Omega_{Ai} = H(\text{ID}_{Ai}, \ell_{Ai})$, and $\varphi_{Ai} = \beta_{Ai} + \Omega_{Ai}.Đ$, where β_{Ai} denotes a random private number that is only know to CA, φ_{Ai} denotes the private key of A_i, and ℓ_{Ai} represents the public key of A_i. At the end, TA can delivers $(\varphi_{Ai}, \ell_{Ai})$ to A_i utilizing secure network.

(iii) Mutual authentication and secrete management: a sender Actor (A_s) with ID_{AS} computes $\mathfrak{S}_{A1_s} = \alpha_{A1_s}.\mathscr{D}$, $\mathfrak{S}_{A2_s} = \alpha_{A2_s}.\mathscr{D}$, $K = \alpha_{A1_s}(\ell_{Ar} + \Omega_{As}\chi)$, and $\text{SKC}_{As} = E_K(\text{ID}_{\text{AS}}, \text{ID}_{\text{AR}})$, where α_{A1_s} and α_{A2_s} represent the two private numbers which are randomly selected by A_s, ℓ_{Ar} denote the public key of receiver actor (A_r), φ_{As} denotes the private key of A_s, and E_K denotes the encryption function that encrypts the identity of A_s and A_r that are $(\text{ID}_{\text{AS}}, \text{ID}_{\text{AR}})$ through the secret key which is generated by A_s. Furthermore, A_s can compute $\xi_{As} = H(\text{ID}_{\text{AS}}, \text{ID}_{\text{AR}})$ and $S_{As} = \alpha_{A2_s} + \xi_{As}.\varphi_{As}$ and send $(\xi_{As}, S_{As}, \mathfrak{S}_{A1_s}, \mathfrak{S}_{A2_s}, \text{SKC}_{As})$ to A_r.

When A_r received $(\xi_{As}, S_{As}, \mathfrak{S}_{A1_s}, \mathfrak{S}_{A2_s}, \text{SKC}_{As})$, it can compute $K = \varphi_{As}.\mathfrak{S}_{A1_s}$, $\text{ID}_{\text{AS}}, \text{ID}_{\text{AR}} = D_K(\text{SKC}_{As})$, and $\xi_{As}/ = H(\text{ID}_{\text{AS}}, \text{ID}_{\text{AR}})$; it compares $\xi_{As}/ = \xi_{As}$; if it is equal, then the identities are not modified, and it is going for signature authentication as $S_{As}.\mathscr{D} = \mathfrak{S}_{A2_s} + \xi_{As}(\beta_{As} + \Omega_{As}.Đ)$ (Table 1).

4.1. Message Signing. A sender Actor (A_s), with ID_{AS}, can compute $\xi_{As} = H(\text{ID}_{\text{AS}}, \text{ID}_{\text{AR}})$ and $S_{As} = \alpha_{A2_s} + \xi_{As}.\varphi_{As}$; α_{A2_s} represents randomly selected by A_s and sends $(S_{As}, \mathfrak{S}_{A2_s})$ to A_r.

4.2. Message Verifications. When A_r received $(S_{As}, \mathfrak{S}_{A2_s})$, it can compute for signature authentication as $S_{As}.\mathscr{D} = \mathfrak{S}_{A2_s} + \xi_{As}(\beta_{As} + \Omega_{As}.Đ)$.

4.3. Correctness. Here, A_r can verify the received set $(\xi_{As}, S_{As}, \mathfrak{S}_{A1_s}, \mathfrak{S}_{A2_s}, \text{SKC}_{As})$ as follows:

$S_{As}.\mathscr{D} = \mathfrak{S}_{A2_s} + \xi_{As}(\ell_{Ai} + \Omega_{Ai}.\chi) = (\alpha_{A2_s} + \xi_{As}.\varphi_{As})\mathscr{D} = (\alpha_{A2_s}\mathscr{D} + \xi_{As}.\varphi_{As}\mathscr{D}) = \mathfrak{S}_{A2_s} + \xi_{As}.(\beta_{As} + \Omega_{As}.Đ)(\mathscr{D} = \mathfrak{S}_{A2_s} + \xi_{As}.(\beta_{As}\mathscr{D} + \Omega_{As}.Đ.\mathscr{D}) = \mathfrak{S}_{A2_s} + \xi_{As}.(\ell_{As} + \Omega_{As}.\chi)$. Hence, it is proved.

Also, it can generate a secret key as $K = \varphi_{As}.\mathfrak{S}_{A1_s} = K = \alpha_{A1_s}(\ell_{As} + \Omega_{As}\chi) = \alpha_{A1_s}(\beta_{As}.\mathscr{D} + \Omega_{As}Đ.\mathscr{D}) = \alpha_{A1_s}.\ \mathscr{D}(\beta_{As} + \Omega_{As}Đ) = \mathfrak{S}_{A1_s}\varphi_{As}$; hence, it is proved.

5. Security Analysis

Before we can describe the security aspects of our proposed scheme, we must first discuss some of the characteristics of an attacker who would represent a threat to it. We will explore the Dolev–Yao model, in which the attacker can conduct a variety of actions. It includes the properties such as mutual authentication, anonymity, confidentiality of identities, unforgeability of signature, forward secrecy, secrete key leakage, and identity authentication. We explain the above properties one by one using the following steps.

Table 1: Symbols used in the proposed algorithm.

Symbol	Used for
χ	Master public key of TA
$Đ$	Master private key of TA
$\mathcal{F}$	Global parameter set
HEC	A genus 2 hyperelliptic curve
A_i	Each actor
E_χ	Represent the encryption function that encrypt the value through the public key of TA
φ_{Ai}	Denotes the private key of A_i
A_s	Sender actor
α_{A1_s}, α_{A2_s}	Represents the two private number which is randomly selected by A_s
ℓ_{Ar}	Denotes the public key of receiver actor (A_r)
E_K	Denotes the encryption function that encrypt the identity of A_s and A_r that are ($\mathrm{ID_{AS}}, \mathrm{ID_{AR}}$) through the secret key which is generated by A_s
TA	Trusted authority
$\mathscr{D}$	A hyperelliptic-curve devisor
H	Collision resistant and one way hash function
F^Q	Denotes an order Q finite field and its value will be equal to 80 bits
ID_{Ai}	Identity of each actor
β_{Ai}	Denotes a random private number that is only know to TA
ℓ_{Ai}	Represents the public key of A_i
$\mathrm{ID_{AS}}$	Identity of sender actor
$\mathrm{ID_{AR}}$	Identity of receiver actor
φ_{As}	Denotes the private key of A_s
K	Common secret key

Table 2: The comparison of computation costs in terms of major operations between schemes in IoV.

Schemes	Message signing	Single message verification	Total
Ali and Li	3 Tmp-ECC + 2Th	Tp + Tmp-ECC + Th	Tp + 4Tmp-ECC + 3Th
Zhong et al.	3 Tmp-ECC + Tmtp + Th	3Tp + Tmtp + 2Tmp-ECC + Tmp-p + Th	3Tp + 2Tmtp + 5Tmp-ECC + Tmp-p + 2Th
Cui et al.	2 Tmp-ECC + 2 Th	Th	2 Tmp-ECC + 3 Th
M.Yao et al.	Tmp-ECC + Th	3Tmp-ECC + 2 Th	4Tmp-ECC + 3 Th
Our scheme	1 Tmp-HECC + Th	3 Tmp-HECC + Th	4Tmp-HECC+ 2Th

5.1. Mutual Authentication. In the proposed scheme, A_s generates a signature as $S_{As} = \alpha_{A2_s} + \xi_{As}.\varphi_{As}$ and sends this signature to A_r through unsecure network. When A_r received S_{As}, for verification, it can check the equality of the following equation $S_{As}.\mathscr{D} = \mathfrak{S}_{A2_s} + \xi_{As}(\beta_{As} + \Omega_{As}.Đ)$; if it is satisfied, then we can say that this scheme provide mutual authentication property. If we look into the correctness analysis section of this study, then we can see the equality of the above equation is hold.

5.2. Anonymity. If we look into the communicated parameter of our proposed scheme ($\xi_{As}, S_{As}, \mathfrak{S}_{A1_s}, \mathfrak{S}_{A2_s}, \mathrm{SKC}_{As}$), where $\xi_{As} = H(\mathrm{ID_{AS}}, \mathrm{ID_{AR}})$ is the hash value with the property of irreversibility, $S_{As} = \alpha_{A2_s} + \xi_{As}.\varphi_{As}$ is the hyperelliptic-curve point which does not contain any identity, $\mathfrak{S}_{A1_s}$ and $\mathfrak{S}_{A2_s}$ are also hyperelliptic-curve point, and $\mathrm{SKC}_{As} = E_K(\mathrm{ID_{AS}}, \mathrm{ID_{AR}})$ in which both the identity of A_s and A_r are protected through encryption function E_K with secret key K that is only known to A_s and A_r. The above discussion confirmed the existence of anonymity property in the proposed scheme.

5.3. Confidentiality of Identities. In the proposed scheme, A_s generate the ciphertext of both the identities is $\mathrm{SKC}_{As} = E_K(\mathrm{ID_{AS}}, \mathrm{ID_{AR}})$ and send it to through unsecure network, where secret key as $K = \alpha_{A1_s}(\ell_{Ar} + \Omega_{As}\chi)$, so if the attacker tries to decrypt the ciphertext, it is obligatory for him/her to make secret key first. However, we need α_{A1_s} from $\mathfrak{S}_{A1_s} = \alpha_{A1_s}.\mathscr{D}$ is equal to find the solution of hyperelliptic-curve discrete logarithm problem that can be infeasible for the attacker.

5.4. Unforgeability of Signature. In the proposed scheme, A_s generate a signature as $S_{As} = \alpha_{A2_s} + \xi_{As}.\varphi_{As}$ and send this signature to A_r through unsecure network. If the attacker tries to make a forge signature, then it will be completely failed because α_{A2_s} and φ_{As} are the two unknown value so that finding two unknown variables from the same equation is infeasible.

5.5. Forward Secrecy. In the proposed scheme, the secret key is renewed for every session so that if the attacker gets access to the previously communicated messages secret key, then it will not be able to extract the content of a currently dispatched message.

5.6. Secrete Key Leakage. When the attacker wants to generate the secret key as $K = \varphi_{As}.\mathfrak{S}_{A1_s}$, then it needs φ_{As} from $\varphi_{Ai} = \beta_{Ai} + \Omega_{Ai}.Đ$ so that it will be completely failed because

Table 3: The comparison of computation costs in terms of milliseconds between schemes in IoV.

Schemes	Message signing	Signature verification	Total
Ali and Li	3*12.4 + 2*0.7 = 38.6	22.4 + 12.4 + 0.7 = 35.5	22.4 + 4*12.4 + 3*0.7 = 74.1
Zhong et al.	3*12.4 + 30.6 + 0.7 = 68.5	3*22.4 + 30.6 + 2*12.4 + 3.1 + 0.7 = 126.4	3*22.4 + 2*30.6 + 5 ∗ 12.4 + 3.1 + 2*0.7 = 194.9
Cui et al.	2*12.4 + 2*0.7 = 26.2	0.7	2*12.4 + 3*0.7 = 26.9
M.Yao et al.	12.4 + 0.7 = 13.1	3*12.4 + 2*0.7 = 38.6	4*12.4 + 3*0.7 = 51.7
Our scheme	1*6.2 + 0.7 = 6.9	3*6.2 + 0.7 = 19.3	4*6.2 + 2*0.7 = 26.2

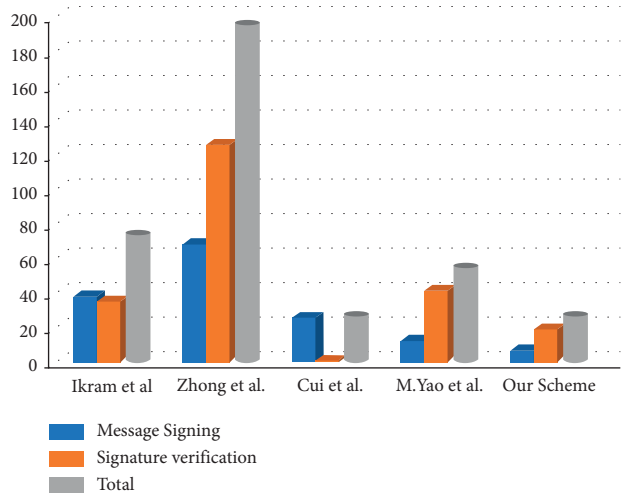

Figure 3: Computational cost comparison in milliseconds.

Table 4: Communicational cost comparisons with the help of major operations.

Schemes	Communication cost	Communication cost with bits
Ali and Li	$\|M\| + 2\|G\| + \|T\|$	1200 + 2*1024 + 34 = 3282 bits
Zhong et al.	$\|M\| + 4\|G\| + \|T\|$	1200 + 4*1024 + 34 = 5330 bits
Cui et al.	$\|M\| + 4\|q\|$	1200 + 4*160 = 1840 bits
M.Yao et al.	$\|M\| + 4\|G\| + \|T\|$	1200 + 4*1024 + 34 = 5330 bits
Our scheme	$\|M\| + 3\|n\|$	1200 + 3*80 = 1440 bits

Note. We suppose $|M| = 1200$ bits, $|T| = 34$ bits, $|G| = 1024$ bits, $|q| = 160$ bits, and $|n| = 80$ bits.

β_{Ai} and $Đ$ are the two unknown values so that finding two unknown variables from the same equation is infeasible.

5.7. Identity Authentication. In the proposed scheme, A_s can encrypt $SKC_{As} = E_K(ID_{AS}, ID_{AR})$ and generate a hash value as $\xi_{As} = H(ID_{AS}, ID_{AR})$; then, send SKC_{As} and ξ_{As} to A_r. When A_r received (ξ_{As}, SKC_{As}), it can compute $\xi_{As}/ = H(ID_{AS}, ID_{AR})$ and then compare $\xi_{As}/ = \xi_{As}$; if it is equal, then the identities are not modified. So, in our scheme, we provide the identity authentication in this way.

6. Computational Cost Comparison

The computational cost is the key component in measuring the cryptographic scheme's performance. Here, we start by defining the notation for the time overhead of some cryptographic operations in the proposed scheme and other schemes that are Ali et al. [24], Zhong et al. [25], Cui et al. [26], and Yao et al. [23]. For this purpose, we then explain that T_h, T_p, T_{mp}-$_p$, T_{mp}-ECC, and T_{mtp} can denote consuming time for a hash function, pairing operation, multiplication over pairing, multiplication over an elliptic curve, and map-to-point operation, respectively. Furthermore, according to [27–29], T_h, T_p, T_{mp}-$_p$, T_{mp}-ECC, and T_{mtp} consume 0.7, 22.4, 3.1, 12.4, and 30.6, respectively. So, Tables 2 and 3 and Figure 3 are witnessed that the proposed scheme required fewer computational costs in the comparisons of Ali et al. [24], Zhong et al. [25], Cui et al. [26], and Yao et al. [23].

7. Communication Overhead

This section compares the proposed scheme's communication overhead efficiencies to those of Ali et al. [24], Zhong et al. [25], Cui et al. [26], and Yao et al. [23]. This comparison is based on extra parameters sent with the message, which are $|T|$, $|G|$, $|q|$, and $|n|$, which represent the current timestamp size, bilinear pairing parameter size, elliptic-curve point size, and hyperelliptic-curve divisor size, respectively.

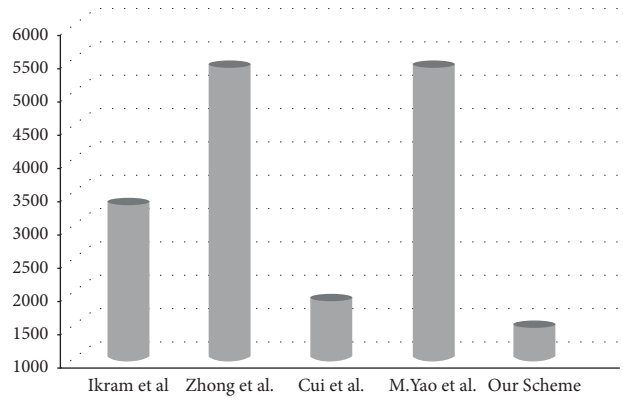

Figure 4: Communication cost comparison in bits.

We assume $|M| = 1200$ bits, $|T| = 34$ bits, $|G| = 1024$ bits, $|q| = 160$ bits, and $|n| = 80$ bits, and we have performed a comparative analysis in Table 4 using these assumed values, which include the extra parameters along with the message in design and Ali et al. [24], Zhong et al. [25], Cui et al. [26], and Yao et al. [23] schemes. We can conclude from Table 3 and Figure 4 that our proposed strategy clearly outperforms the other four designs in both characteristics.

8. Conclusion

This study proposed a low-cost, privacy-preserving authentication and key management strategy for the IoV ecosystem. The proposed solution makes use of the HECC mathematical concept. In terms of computation and communication costs, the proposed scheme is more cost-effective than existing privacy-preserving authentication solutions. Mutual authentication, anonymity, identity confidentiality, signature unforgeability, forward secrecy, secret key leakage, and identity authentication are among the security properties offered by the proposed approach. As a consequence, because the HECC has fewer parameters and delivers the same level of security as the elliptic curve and RSA, the proposed scheme may be a better alternative for IoV system.

Data Availability

All the data are used to support the findings of the study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the present study.

References

[1] M. Umar, S. H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar, and M. A. Saleem, "Provable secure identity-based anonymous and privacy-preserving inter-vehicular authentication protocol for VANETS using PUF," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12158–12167, 2021.

[2] 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 Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[3] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in IoV," *IEEE Systems Journal*, vol. 15, no. 1, pp. 245–256, 2021.

[4] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance," *Journal of Systems Architecture*, vol. 115, Article ID 101955, 2021.

[5] I. Ullah, M. A. Khan, F. Khan et al., "An efficient and secure multi-message and multi-receiver signcryption scheme for edge enabled Internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, pp. 2688–2697, 2021.

[6] M. N. Majeed, S. P. Chattha, A. Akram, and M. Zafrullah, "Vehicular ad hoc networks: history and future development arenas," *Int. J. Inf. Techno. Elect. Eng.*vol. 2, no. 2, pp. 25–29, 2013.

[7] D. Kombate, "December the Internet of vehicles based on 5G communications," in *Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 445–448, IEEE, Chengdu, China, December 2016.

[8] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.

[9] N. Sharma, N. Chauhan, and N. Chand, "Security challenges in internet of vehicles (IoV) environment," in *Proceedings of the 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pp. 203–207, IEEE, Jalandhar, India, December 2018.

[10] 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 Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, 2017.

[11] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, K. K. R. Choo, and Y. Park, "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1736–1751, 2021.

[12] M. Zhang, J. Zhou, G. Zhang, M. Zou, and M. Chen, "EC-BAAS: elliptic curve-based batch anonymous authentication scheme for Internet of Vehicles," *Journal of Systems Architecture*, vol. 117, Article ID 102161, 2021.

[13] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 1229–1237, IEEE, Phoenix, AZ, USA, April 2008.

[14] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 246–250, IEEE, Phoenix, AZ, USA, April 2008.

[15] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE*

Transactions on Intelligent Transportation Systems, vol. 17, no. 8, pp. 2193–2204, 2016.

[16] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: a two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896–911, 2016.

[17] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.

[18] 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, 2018.

[19] P. Liu, B. Liu, Y. Sun, B. Zhao, and I. You, "Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," *IEEE Access*, vol. 6, Article ID 20806, 2018.

[20] G. Raja, S. Anbalagan, G. Vijayaraghavan, P. Dhanasekaran, Y. D. Al-Otaibi, and A. K. Bashir, "Energy-efficient end-to-end security for software-defined vehicular networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5730–5737, 2021.

[21] M. Hashem Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 7868–7881, 2016.

[22] S. Bouchelaghem and M. Omar, "Secure and efficient pseudonymization for privacy-preserving vehicular communications in smart cities," *Computers & Electrical Engineering*, vol. 82, Article ID 106557, 2020.

[23] M. Yao, X. Wang, Q. Gan, Y. Lin, and C. Huang, "An Improved and Privacy-Preserving Mutual Authentication Scheme with Forward Secrecy in VANET," *Security and Communication Networks*, vol. 2021, Article ID 6698099, 12 pages, 2021.

[24] I. Ali, T. Lawrence, A. A. Omala, and F. Li, "An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, Article ID 11280, 2020.

[25] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Information Sciences*, vol. 476, pp. 211–221, 2019.

[26] J. Cui, W. Xu, Y. Han, J. Zhang, and H. Zhong, "Secure mutual authentication with privacy preservation in vehicular ad hoc networks," *Vehicular Communications*, vol. 21, Article ID 100200, 2020.

[27] M. A. Khan, I. Ullah, M. H. Alsharif, A. H. Alghtani, A. A. Aly, and C. M. Chen, "An Efficient Certificate-Based Aggregate Signature Scheme for Internet of Drones," *Security and Communication Networks*, vol. 2022, Article ID 9718580, 9 pages, 2022.

[28] M. A. Khan, H. Shah, S. U. Rehman et al., "Securing internet of drones with identity-based proxy signcryption," *IEEE Access*, vol. 9, Article ID 89142, 2021.

[29] I. Ullah, S. Zeadally, N. U. Amin, M. K. Asghar, and H. Khattak, "Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN)," *Microprocessors and Microsystems*, vol. 81, Article ID 103477, 2021.