Manchester Metropolitan University

e-space

Manchester Metropolitan University's Research Repository

Please cite the Published Version

Iqbal, Asad, Ullah, Insaf, AlSanad, Abeer Abdulaziz, Ul Haq, Muhammad Inam, Khan, Muhammad Asghar, Khan, Wali Ullah and Rabie, Khaled (2022) A cost-effective identity-based signature scheme for vehicular ad hoc network using hyperelliptic curve cryptography. Wireless Communications and Mobile Computing, 2022. p. 5012770. ISSN 1530-8669

DOI: https://doi.org/10.1155/2022/5012770

Publisher: Hindawi

Version: Published Version

Downloaded from: https://e-space.mmu.ac.uk/629866/

Usage rights: Creative Commons: Attribution 4.0

Additional Information: This is an Open Access article which appeared in Wireless Communications and Mobile Computing, published by Hindawi. This article is part of the Special Issue "Recent Advances in Physical Layer Technologies for 5G-Enabled Internet of Things 2022"

Data Access Statement: All the data is presented in this paper.

Enquiries:
If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines)

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5012770, 8 pages
https://doi.org/10.1155/2022/5012770

Research Article

A Cost-Effective Identity-Based Signature Scheme for Vehicular Ad Hoc Network Using Hyperelliptic Curve Cryptography

Asad Iqbal,[1] Insaf Ullah,[2] Abeer Abdulaziz AlSanad,[3] Muhammad Inam Ul Haq,[1] Muhammad Asghar Khan,[2] Wali Ullah Khan,[4] and Khaled Rabie[5]

[1]*Department of Computer Science and Bioinformatics, Kushal Khan Khattak University Karak, 27200, Karak Khyber Pakhtunkhwa, Pakistan*
[2]*Hamdard Institute of Engineering & Technology, Hamdard University, Islamabad 44000, Pakistan*
[3]*Information Systems Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh 11432, Saudi Arabia*
[4]*Interdisciplinary Center for Security, Reliability and Trust (SnT), University of Luxembourg, 1855 Luxembourg City, Luxembourg*
[5]*Department of Engineering, Manchester Metropolitan University, Manchester, UK*

Correspondence should be addressed to Muhammad Asghar Khan; khayyam2302@gmail.com

Received 13 March 2022; Revised 16 April 2022; Accepted 23 April 2022; Published 12 May 2022

Academic Editor: Chi-Hua Chen

Copyright © 2022 Asad Iqbal et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A Vehicular Ad Hoc Network (VANET) is a subset of the Mobile Ad Hoc Network (MANET) that allows vehicles to communicate with each other and with roadside stations to offer efficient and safe transportation. Furthermore, when VANET is used in connection with the Internet of Things (IoT) devices and sensors, it can help with traffic management and road safety by allowing vehicles to interact with one another at any time and from any location. Since VANET's event-driven communications are carried out via an open wireless channel, there are significant security concerns. In this paper, we use Hyperelliptic Curve Cryptography (HECC) to offer a cost-effective identity-based signature for secure communication over VANET. The proposed scheme does not need certificate management, and we found that it is more secure against a variety of cryptographic threats after conducting a thorough security analysis. In addition, comparisons of communication and computational costs are made, demonstrating that the proposed scheme is more efficient in both respects than existing schemes.

1. Introduction

Vehicular Ad Hoc Networks (VANETs) have lately received a lot of attention and are now regarded as an important aspect of the automotive sector. VANET is being utilized in the Intelligent Transportation System (ITS) to aid passenger vehicles and infrastructure with issues like road safety, issuing misadventure alerts and assisting drivers, and offering other entertainment services [1]. By integrating Internet of Things (IoT) applications with intelligent transportation mechanisms, VANET creates a secure environment for vehicle communication [2]. The general architecture for VANET is shown in Figure 1, which comprises cars with built-in onboard units (OBUs), Road-Side Units (RSUs), and Trusted Authority (TA). The OBU's job is to connect with surrounding vehicles and RSUs through an open wireless channel, such as the Dedicated Short Range Communication (DSRC) protocol [3]. RSUs are antennas that are placed along the side of the road to collect traffic-related data from automobiles, while TA is a high-performance computing and storage entity in charge of numerous VANET applications including registration and key generation for OBU and RSU [4].

The VANET supports three forms of communication: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-infrastructure (I2I). Open Dedicated Short Range Radio Signals (DSRS) are used for V2V communication, whereas secure channels are used for V2I and I2I communication [5, 6]. Each vehicle in the VANET connects with nearby vehicles and RSUs through OBU,

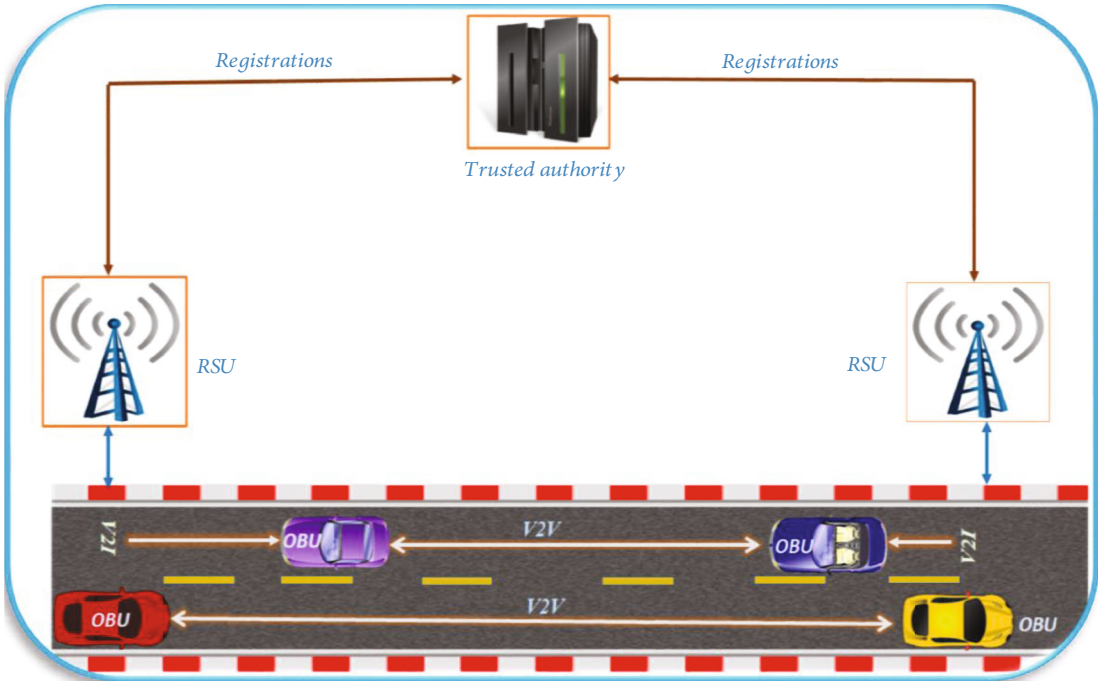

Figure 1: Flow model for VANET.

providing traffic-related information such as position, speed, current time, and traffic and road conditions [5–7].

Because VANET communication could take place over an open wireless channel, authentication is a major concern [8]. Digital signatures will be the most appropriate solution for dealing with this type of situation. It allows a VANET sender node to produce a signature on a dispatchable document using his private key and then transfer it over to the receiver node. The recipient node validates the signature using the sender's public key after getting it. Though digital signatures are based on asymmetric key cryptography, the first candidate is Public Key Infrastructure (PKI), in which the Certificate Authority (CA) presents the user with a certificate. The main disadvantage of PKI is certificate management. PKI is being phased out in favour of identity-based cryptography, which does not require certificate management. In this cryptosystem, users just provide their identities to TA, which subsequently produces the public and private keys for that identity and sends them through a secure channel.

Rivest-Shamir-Adleman (RSA), bilinear pairing (BP), and Elliptic Curve Cryptography (ECC) are commonly employed to achieve security and efficiency in security schemes. These algorithms are frequently based on computationally difficult problems. With a key size of up to 1024 bits, RSA cryptography employs enormous factorization [9]. Due to huge pairing and map-to-point function calculation, BP is 14.31 times worse than RSA. ECC, a modern cryptography method, was utilized to address the difficulties in RSA and BP with a key size up to 160 bits, reducing the computationally difficult problem to some extent, but it is still not supported by resource-constrained devices. A new cryptographic system called Hyperelliptic Curve Cryptography (HECC) was created for this purpose, and it provides the same level of security as EC [10]. While giving the security features of RSA, BP, and ECC, the HECC employs an 80-bit key size. The HECC is an excellent starting point for a VANET system.

1.1. Preliminaries. The HECC can be defined as the following: it is a generalized form of elliptic curves and state $W(Tq)$ over finite field F_q defined by equation $W : b^2 + h(a)b = t(a) \bmod q$, where $h(a) \in T[a]$ is a polynomial and degree $h(a) \leq g$ and $t(a) \in T[a]$ is a monic polynomial and degree $t(a) \leq 2g + 1$. further, it includes devisor which is a finite formal sum of points, and according to Mumford, it can be represented as $S = (x(a), y(a)) = (\sum_{i=0}^{g} x_i a^i, \sum_{i=0}^{g-1} y_i a^i)$. The divisors form an Abelian group which is called Jacobian group $J_c(T_q)$, and the order of the Jacobian group $o(J_c(T_q))$ is defined as $|(\sqrt{q} - 1)^{2g}| \leq o(J_c(T_q)) \leq |(\sqrt{q} + 1)^{2g}|$. So, the whole security of the hyperelliptic curve cryptosystem is based on the hyperelliptic curve discrete logarithm problem, which can be defined as the following: Let S be a divisor of order n in the Jacobian group $J_c(T_q)$, find an integer $a \in T_q$, such that $S_1 = a \cdot S$.

1.2. Motivation and Contributions. So, inspired by the idea of HECC, we make the following contribution to this work as a result of the preceding discussion:

(1) We propose a batch verification method based on HECC using authentication and key management mechanism

(2) We carried out a thorough security analysis and confirmed that the proposed scheme is resistant to a variety of cyberattacks

(3) By comparing the proposed scheme to a previously published scheme, we performed a cost analysis study in terms of both communication and computation, and the findings show that the proposed scheme is efficient

2. Literature Review

VANET is a network that allows vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication (V-I). VANET communication, on the other hand, uses the Internet, necessitating the need for authentication procedures to avoid rogue nodes. One of the better options is to employ digital signatures, which allow a sender to create a digital signature on data created in a VANET environment using his private key and then deliver it to the receiver. Using the sender's public key, the receiver may easily verify the signature after receiving it [11]. As a result, various academics have developed digital signature systems for traffic-related communications in VANET authentication.

Raya and Hubaux [12] proposed a Public Key Infrastructure- (PKI-) based authentication technique in which the Certificate Authority (CA) generates a large number of anonymous private/public keys and certificates in a short period of time to sign traffic-related communications. However, because of the limited storage capacity of the vehicle's OBU, it is not ideal for storing a pair of large numbers of public/private keys and certificates. On the basis of anonymous certificates, Lu et al. [13] enhanced the system used in [12] and contributed a new Conditional Privacy Preservation Authentication (CPPA) scheme.

This scheme is not appropriate for real-time communication systems due to certificate renewal issues. Freudiger et al. [14] offered another authentication approach in which they integrated the mix zone and anonymous certificate methods. However, when a high number of certificates are required, it has an impact on RSU's storage capacity. Zhang et al. [15] proposed an efficient authentication technique that included the use of Hash Message Authentication Codes (HMAC) to ensure privacy preservation. For connecting with RSU, a random public/private key pair and certificate were assigned in this scheme. However, cars are still obliged to hold the maximum amount of certificates under this approach, which solves the storage problem. Wasef and Shen [16] suggested another PKI-based approach, the Expedite Message Authentication Protocol (EMAP). By replacing the Certificate Revocation List (CRL) with keyed HMAC, they were able to speed up the revocation checking procedure.

By employing bilinear pairing, Zhang et al. [17] proposed a CPPA signature technique based on identity for VANETs. By combining the feature of group signature with batch verification and bilinear pairing, Chim et al. [18] created an identity-based technique. For V2V communication, Shim [19] presented an identity-based CPPA signature technique based on bilinear pairing. Horng et al. [20] created an ID-based signature technique for VANETs that uses bilinear pairing and also supports batch signatures. However, the techniques in [17–21] may have an impact on real-time communication since they are based on bilinear pairing, which necessitates higher channel capacity and processing resources. Sun et al. [21] designed the CPPA signature, by utilizing bilinear pairing. However, this scheme can affect real-time communication as it is based on bilinear pairing that must need greater capacity in the channel and more computational power. He et al. [22] proposed a new ID-based CPPA signature system for both V2V and V2I communication in VANET with the use of ECC. This scheme's results showed that it was successful in facilitating batch signature verification and assessing VANET in high-traffic locations. However, throughout the three-point multiplication operation, there was a delay in confirming signatures. Using ECC, Ikram et al. presented an ID-based signature technique for V2V communication on VANETs. Their technique, however, still has a significant computational overhead.

3. Network Model

Figure 2 depicts the network model for the proposed method, which includes three entities: onboard units (OBUs), roadside units (RSUs), and the Department of Transportation (DoT). The steps to take are as follows:

(1) *OBU*. It has 5G technology and can connect with other OBUs, as well as DoT and RSU. Its duty also includes registering with DoT by transmitting his identification; after DoT receives his identity, DoT generates the public and private keys for his identity and delivers them to the OBU. Then, utilizing an open network, OBU may build data signatures and transfer them to RSU.

(2) *RSU*. It is a 5G-enabled base station in charge of V-I communication management and execution. Its duty also includes registering with DoT by transmitting his identification; after DoT receives his identity, DoT generates the public and private keys for his identity and sends it back to the RSU. Furthermore, when RSU receives signed data from OBU, it performs a verification procedure; if the signature is acceptable, the message is accepted; otherwise, an error message is generated.

(3) *DoT*. The DoT is a trustworthy third party with significant computational and storage power. It establishes system parameters and makes them publicly available to other organizations. When DoT receives OBU and RSU's identities, it generates public and private keys and sends them to OBU and RSU separately.

4. Proposed Scheme

The proposed batch verification identity-based signature can be executed through the steps that are explained below. Before we start the proposed algorithm, in Table 1, the symbols used during its constructions are explained.

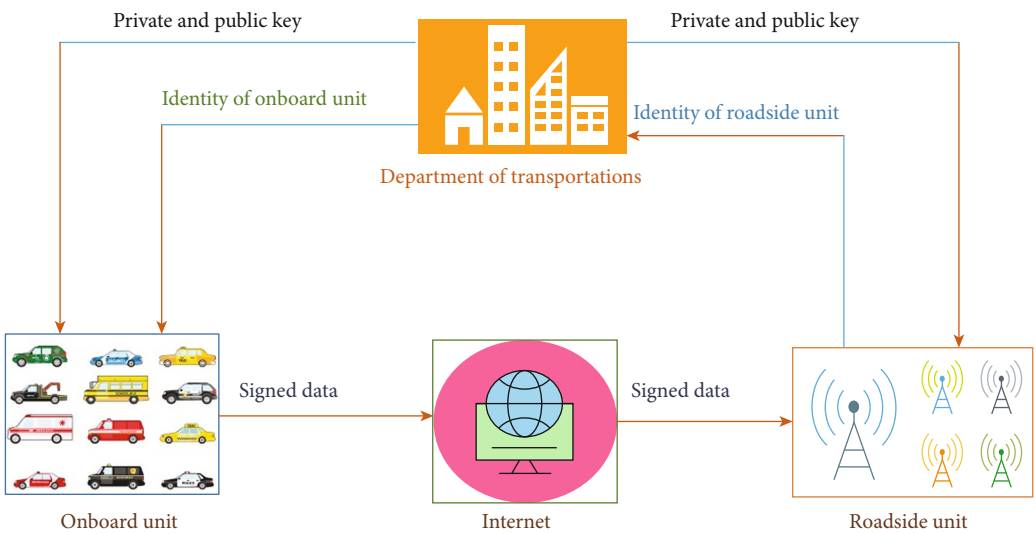

Figure 2: Network model for proposed scheme.

Table 1: Symbols used in the proposed algorithm.

Symbol	Description
λ	It is used to indicate security parameter
H	Denotes the hash function like SHA 256 which avoids the reversed manner
χ	Denotes the private key of TA
ID_{V}	Denotes the identity for each vehicle in the system
Ω_{rv}	The private key for receiver vehicle
ζ_{sv}	The public key for sender vehicle
$\mathrm{ID}_{\mathrm{rV}}$	The identity for receiver vehicle
δ	Indicates the public key of TA
$\mathbf{F}_n$	Denotes the nonfinite field of hyperelliptic curve
$\mathscr{D}$	Denotes devisor of hyperelliptic curve
Ω_{sv}	The private key for sender vehicle
$\mathrm{ID}_{\mathrm{sV}}$	The identity for sender vehicle
ζ_{rv}	The public key for receiver vehicle
M	Indicates the plaintext

Setup: this algorithm is processed by Trusted Authority (TA) when it receives the security parameter $\lambda = 80$ bits in size; further, it selects χ as his private key and executes his public key as $\delta = \chi \cdot \mathscr{D}$. Moreover, TA published the set $\gamma = \{\delta, \mathscr{D}, \mathbf{F}_n, H\}$, where $\mathbf{F}_n$ and H denotes the nonfinite field of the hyperelliptic curve and hash function like SHA 256 which avoids the reversed manner.

Key generation: for a vehicle with identity (ID_{V}), TA compute the public and private keys as follows:

(i) Compute $\zeta_{\mathrm{v}} = \alpha_{\mathrm{v}} \cdot \mathscr{D}$, where α_{v} is the secret number from $\mathbf{F}_n$

(ii) Compute $\xi = H(\zeta_{\mathrm{v}}, \mathrm{ID}_{\mathrm{V}})$ and $\beta = \xi \cdot \delta$

(iii) Compute $\Omega_{\mathrm{v}} = \alpha_{\mathrm{v}} + \xi \cdot \chi$ and send $\zeta_{\mathrm{v}}, \Omega_{\mathrm{v}}$, and β as a public key, private key, and public number to ID_{V}

Signature generation: a sender vehicle with identity ($\mathrm{ID}_{\mathrm{sV}}$) can sign the received data from OBU as follows.

(i) Compute $\ell = \upsilon \cdot \mathscr{D}$, where υ is the secret number from $\mathbf{F}_n$

(ii) Compute $\mathfrak{S} = H(M, \ell, \mathrm{ID}_{\mathrm{sV}})$ and $\mathscr{J} = \upsilon + \mathfrak{S} \cdot \Omega_{\mathrm{sv}}$

(iii) Set $(\mathscr{J}, \ell)$ as a signature pair and send it to the receiver vehicle

Signature verifications: a receiver vehicle with identity ($\mathrm{ID}_{\mathrm{rV}}$) can verify the received signature pair $(\mathscr{J}, \ell)$ as

Table 2: Computational cost comparisons with respect to major operations and ms.

Schemes	Signing cost	Verification cost	Total cost (in ms)
Ali et al. [25]	3 ERM	1 ERM	$4 * 0.97 = 3.88$
Lo and Tsai [26]	2 ERM	2 ERM	$4 * 0.97 = 3.88$
He et al. [22]	4 ERM	3 ERM	$7 * 0.97 = 6.79$
Wang and Yao [27]	1 BPRM	3 BP	$1 * 4.31 + 3 * 14.90 = 49.01$
Bayat et al. [28]	5 BPRM	3 BP	$5 * 4.31 + 3 * 14.90 = 66.25$
Jianhong et al. [29]	5 BPRM	3 BP	$5 * 4.31 + 3 * 14.90 = 66.25$
Proposed	2HERM	2HERM	$4 * 0.48 = 1.92$

follows: it computes $\mathfrak{S} = H(M, \ell, \mathrm{ID}_{\mathrm{sV}})$ and accepts $(\mathcal{J}, \ell)$ when $\mathcal{J} \cdot \mathcal{D} = \ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \beta)$ are satisfied.

Batch signature generation: a sender vehicle with identity $(\mathrm{ID}_{\mathrm{sV}})$ can sign the batch data of OBU as follows.

(i) Compute $\mathcal{G} = \sum_{i=0}^{n} \ell$ and $\mathcal{C} = \sum_{i=0}^{n} \mathcal{J}$

(ii) Set $(\mathcal{C}, \mathcal{G})$ as a batch signature pair and send it to the receiver vehicle

Batch signature verifications: a receiver vehicle with identity $(\mathrm{ID}_{\mathrm{rV}})$ can verify the received batch signature pair $(\mathcal{C}, \mathcal{G})$ as follows: it computes $\mathfrak{S} = H(M, \ell, \mathrm{ID}_{\mathrm{sV}})$ and accepts $(\mathcal{C}, \mathcal{G})$ when $\sum_{i=0}^{n} \mathcal{J} \cdot \mathcal{D} = \sum_{i=0}^{n} \ell + \mathfrak{S} \cdot \sum_{i=0}^{n} (\zeta_{\mathrm{sv}} + \beta)$ are satisfied.

4.1. Correctness. The signature verification can be done as is $\mathcal{J} \cdot \mathcal{D} = \ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \beta)$ satisfied $\mathcal{J} \cdot \mathcal{D} = (\upsilon + \mathfrak{S} \cdot \Omega_{\mathrm{sv}}) \cdot \mathcal{D} = (\upsilon \cdot \mathcal{D} + \mathfrak{S} \cdot \Omega_{\mathrm{sv}} \cdot \mathcal{D}) = (\upsilon . \mathcal{D} + \mathfrak{S} \cdot (\alpha_{\mathrm{sv}} + \xi \cdot \chi) \cdot \mathcal{D}) = (\ell + \mathfrak{S} \cdot ((\alpha_{\mathrm{sv}} \cdot \mathcal{D} + \xi \cdot \chi \cdot \mathcal{D})) = (\ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \xi \cdot \chi \cdot \mathcal{D})) = (\ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \xi \cdot \delta)) = (\ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \beta)) = \mathcal{J} \cdot \mathcal{D}$ hence proved.

Also, the batch signature verification can be done as is $\sum_{i=0}^{n} \mathcal{J} \cdot \mathcal{D} = \sum_{i=0}^{n} \ell + \mathfrak{S} \cdot \sum_{i=0}^{n} (\zeta_{\mathrm{sv}} + \beta)$ are satisfied.

$\sum_{i=0}^{n} \mathcal{J} \cdot \mathcal{D} = \sum_{i=0}^{n} (\upsilon + \mathfrak{S} \cdot \Omega_{\mathrm{sv}}) \cdot \mathcal{D} = \sum_{i=0}^{n} (\upsilon \cdot \mathcal{D} + \mathfrak{S} \cdot \Omega_{\mathrm{sv}} \cdot \mathcal{D}) = \sum_{i=0}^{n} (\upsilon \cdot \mathcal{D} + \mathfrak{S} \cdot (\alpha_{\mathrm{sv}} + \xi \cdot \chi) \cdot \mathcal{D}) = \sum_{i=0}^{n} (\ell + \mathfrak{S} \cdot ((\alpha_{\mathrm{sv}} \cdot \mathcal{D} + \xi \cdot \chi \cdot \mathcal{D})) = \sum_{i=0}^{n} (\ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \xi \cdot \chi \cdot \mathcal{D})) = \sum_{i=0}^{n} \ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \xi \cdot \delta)) = \sum_{i=0}^{n} (\ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \beta)) = \sum_{i=0}^{n} \sum_{i=0}^{n} \mathcal{J} \cdot \mathcal{D}$ hence proved.

5. Security Analysis

Before going to discuss the security properties, we must discuss some properties of an attacker that can be a threat to our proposed scheme. Here, we consider the Dolev-Yao model, in which the attacker can perform interception and impersonation, break the privacy of identity, break the process of mutual authentication, and can generate a forged signature, respectively. In the following subphases, we have proved that our designed approach can resist various cyberattacks.

5.1. Authentication. For the authentication, the sender computes $\mathcal{J} = \upsilon + \mathfrak{S} \cdot \Omega_{\mathrm{sv}}$ and sends it to the receiver. After the reception of $\mathcal{J}$, the receiver computes $\mathfrak{S} = H(M, \ell, \mathrm{ID}_{\mathrm{sV}})$ and accepts $(\mathcal{J}, \ell)$ when $\mathcal{J} \cdot \mathcal{D} = \ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \beta)$ are satisfied, so that our scheme meets the authentication security service in this way.

5.2. Identity Privacy Preservation. The identity privacy preservation can be done in the proposed scheme in a way that we are not sending any user identity in an open channel during communication between two devices in VANET. We only send $(\mathcal{J}, \ell)$ in an open network, where $\mathcal{J} = \upsilon + \mathfrak{S} \cdot \Omega_{\mathrm{sv}}$ and $\ell = \upsilon \cdot \mathcal{D}$, so it is obvious that it does not contain any user identity.

5.3. Nonrepudiation. A vehicle or RSU in VANET should not be able to refuse any traffic-related message sent by it, because it used its private key during signature generation $(\mathcal{J} = \upsilon + \mathfrak{S} \cdot \Omega_{\mathrm{sv}})$ which is directly associated with its public key. So, the receiver or TA can verify the received signature by using $\mathcal{J} \cdot \mathcal{D} = \ell + \mathfrak{S} \cdot (\zeta_{\mathrm{sv}} + \beta)$; if this equation holds, then TA can decide the message from the sender.

5.4. Traceability. If a malicious vehicle transmits a false traffic-related message, only the TA can trace the vehicle's original identity. In our proposed scheme, let us say if the malicious vehicle with identity $(\mathrm{ID}_{\mathrm{mV}})$ can generate a signature on a false as the following: it computes $\ell = \upsilon \cdot \ ?$, $\mathfrak{S} = H(M, \ell, \mathrm{ID}_{\mathrm{mV}})$, $\mathcal{J} = \upsilon + \mathfrak{S} \cdot \Omega_{\mathrm{mv}}$, and sends a tuple $(\mathcal{J}, \ell)$ as a signature pair to the receiver vehicle. A receiver vehicle with identity $(\mathrm{ID}_{\mathrm{rV}})$ can verify the received signature pair $(\mathcal{J}, \ell)$ as follows: it computes $\mathfrak{S} = H(M, \ell, \mathrm{ID}_{\mathrm{mV}})$ and accepts $(\mathcal{J}, \ell)$ when $\mathcal{J} \cdot \mathcal{D} = \ell + \mathfrak{S} \cdot (\zeta_{\mathrm{mv}} + \beta)$ are satisfied. So, if the receiver found that the message signature which was sent by the malicious sender is harmful, then it reports this vehicle identity to the TA, and TA backlists this identity for the future.

5.5. Impersonation Attack. The proposed mechanism avoids this attack because it transmits only two parameters $(\mathcal{J}, \ell)$, which will be the obligatory need for the attacker to impersonate the signature, where ℓ is the public number which can easily be accessible for the attacker and $= \upsilon + \mathfrak{S} \cdot \Omega_{\mathrm{mv}}$, so for this, the attacker needs υ from $\ell = \upsilon \cdot \mathcal{D}$ which cannot be feasible because of the hard nature of the hyperelliptic curve discrete logarithm problem. Further, the attacker desires to make $\Omega_{\mathrm{v}} = \alpha_{\mathrm{v}} + \xi \cdot \chi$, which further requires α_{v} from $\zeta_{\mathrm{v}} = \alpha_{\mathrm{v}} \cdot \mathcal{D}$ and χ from $\delta = \chi \cdot \mathcal{D}$, which cannot be feasible because of the two-time hard nature of the hyperelliptic curve discrete logarithm problem.

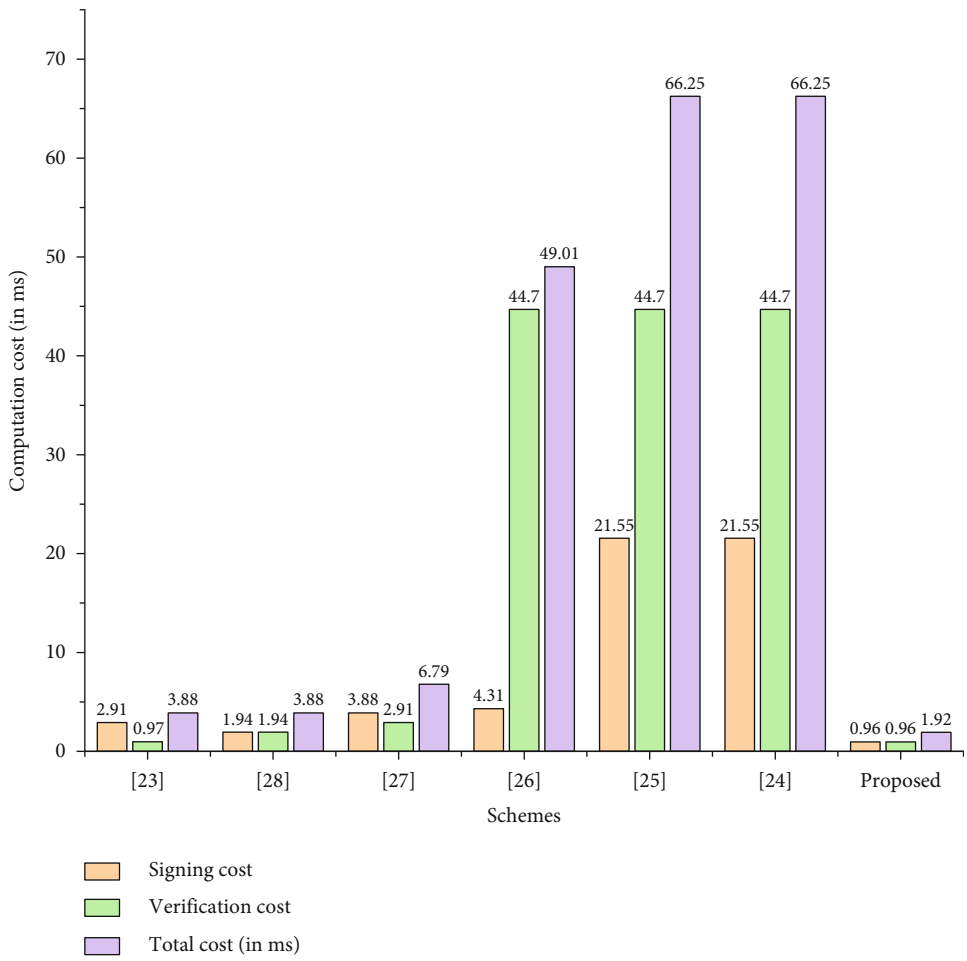

Figure 3: Comparison of computational cost.

5.6. Modification Attack. The attacker cannot modify the signature tuple; it needs υ from $\ell = \upsilon \cdot \mathscr{D}$ which cannot be feasible because of the hard nature of the hyperelliptic curve discrete logarithm problem. Further, the attacker desires to make $\Omega_v = \alpha_v + \xi \cdot \chi$, which further requires α_v from $\zeta_v = \alpha_v \cdot \mathscr{D}$ and χ from $\delta = \chi \cdot \mathscr{D}$, which cannot be feasible because of the two-time hard nature of the hyperelliptic curve discrete logarithm problem.

6. Computational Cost

In this section, we compare our proposed scheme with existing schemes in terms of computational cost. Typically, the computational cost involves heavy mathematical operations. Our scheme has been compared with three bilinear pairing (BP) schemes as well as three elliptic curves (EC), which involve heavy computation. We measure computational cost in milliseconds (ms) for comparison. The single Elliptic Curve Point Multiplication (ERM) needs 0.97 ms, Bilinear Pairing Point Multiplication (BPRM) takes 4.31 ms, and BP take 14.90 ms [23, 24]. We utilize hyperelliptic curve divisor multiplications (HERM) [10] that take 0.48 ms to process and use a half amount of key, i.e., 80 bits as compared to EC, which provides the same level of security. According to Table 2 and Figure 3, in which we have provided the comparisons of the proposed and existing schemes with the help of major operations and milliseconds, our scheme is more efficient than existing schemes.

Table 3: Communication cost analysis between proposed scheme and existing schemes on the basis of bits.

Schemes	Communication cost	Communication cost with bits
Ali et al. [25]	$\|m\| + 2\|q\|$	$850 + 2 * 160 = 1170$ bits
Lo and Tsai [26]	$\|m\| + 3\|q\|$	$850 + 3 * 160 = 1330$ bits
He et al. [22]	$\|m\| + 4\|q\|$	$850 + 4 * 160 = 1490$ bits
Wang and Yao [27]	$\|m\| + 3\|G\|$	$850 + 3 * 1024 = 3922$ bits
Bayat et al. [28]	$\|m\| + 3\|G\|$	$850 + 3 * 1024 = 3922$ bits
Jianhong et al. [29]	$\|m\| + 3\|G\|$	$850 + 3 * 1024 = 3922$ bits
Proposed	$\|m\| + 2\|n\|$	$850 + 2 * 80 = 1010$ bits

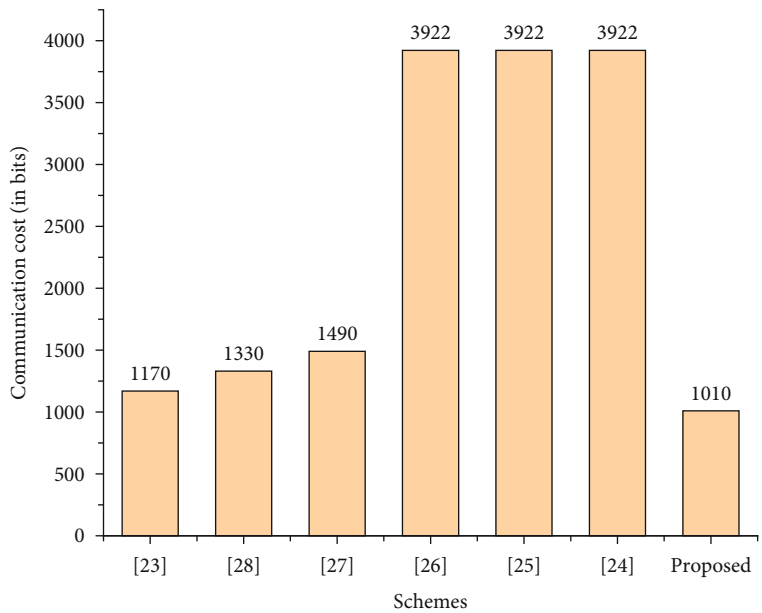

Figure 4: Comparison of communication cost.

The observation is produced from a workstation having the following specification.

(i) Intel Core i5-6300 CPU

(ii) 2.40 GHz processor

(iii) 8 GB of RAM

(iv) Windows 10 Ultimate edition

7. Communication Overhead

In this section, our proposed scheme has been compared with Ali et al. [25], Lo and Tsai [26], He et al. [22], Wang and Yao [27], Bayat et al. [28], and Jianhong et al. [29] in terms of communication overhead. For this purpose, we consider $|m|$ as the plaintext, and its size is supposed to be equal to 850 bits; $|G|$ for bilinear pairing, where its size in bits is 1024; $|q|$ for elliptic curve where its size in bits is 160; and $|n|$ for hyperelliptic curve where its size in bits is 80, respectively. Therefore, it is clear from Table 3 and Figure 4 that our scheme is superior in communicational overhead to the schemes proposed in [22, 25–29].

8. Conclusion

In this paper, we proposed a cost-effective identity-based signature for the deployment of VANET using Hyperelliptic Curve Cryptography (HECC) to lower the computational cost of verifying vehicles during message authentication. The proposed scheme supports a batch signature verification approach, which allows each vehicle in a high-traffic area to validate multiple messages at the same time. Authentication, identity privacy preservation, nonrepudiation, traceability, impersonation attack, and modification attack are all security criteria that the proposed technique meets. Our research demonstrates that the proposed scheme will be a preferable choice for VANET in terms of computational and communicational cost when compared to current similar techniques.

Data Availability

All the data is presented in this paper.

Conflicts of Interest

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

References

[1] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: challenges and countermeasures," *Security and Communication Networks*, vol. 2021, 20 pages, 2021.

[2] S. M. Hatim, S. J. Elias, N. Awang, and M. Y. Darus, "VANETs and Internet of Things (IoT): a discussion," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 1, pp. 218–224, 2018.

[3] B. P. Roberts and C. Sandberg, "The role of energy storage in development of smart grids," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1139–1144, 2011.

[4] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[5] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Information Sciences*, vol. 451-452, pp. 1–15, 2018.

[6] W. Khan, T. N. Nguyen, F. Jameel et al., *Learning-Based Resource Allocation for Backscatter-Aided Vehicular Networks*, TechRxiv. Preprint, 2021.

[7] W. U. Khan, A. Ihsan, T. N. Nguyen, M. A. Javed, and Z. Ali, "NOMA-enabled backscatter communications for green transportation in automotive-Industry 5.0," *IEEE Transactions on Industrial Informatics*, 2022.

[8] 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.

[9] M. A. Khan, I. Ullah, S. Nisar et al., "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.

[10] I. Ullah, M. A. Khan, M. H. Alsharif, and R. Nordin, "An anonymous certificateless signcryption scheme for secure and efficient deployment of internet of vehicles," *Sustainability*, vol. 13, no. 19, p. 10891, 2021.

[11] S. F. Tzeng, C. Y. Yang, and M. S. Hwang, "A new digital signature scheme based on factoring and discrete logarithms," *International Journal of Computer Mathematics*, vol. 81, no. 1, pp. 9–14, 2004.

[12] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

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

[14] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J. P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proc. 1st Int. Workshop on Wireless Netw. Intell. Transp. Syst.*, Vancouver, BC, Canada, 2007.

[15] C. Zhang, X. Lin, R. Lu, and P. H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks," in *2008 IEEE international conference on communications*, pp. 1451–1457, 2008.

[16] A. Wasef and X. Shen, "EMAP: expedite message authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 78–89, 2013.

[17] C. Zhang, P. H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17, no. 8, pp. 1851–1865, 2011.

[18] T. W. Chim, S. M. Yiu, L. C. Hui, and V. O. Li, "SPECS: secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189–203, 2011.

[19] K. A. Shim, "CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012.

[20] S. J. Horng, S. F. Tzeng, Y. Pan et al., "b-SPECS+: batch verification for secure pseudonymous authentication in VANET," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

[21] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[22] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[23] M. A. Khan, H. Shah, S. U. Rehman et al., "Securing internet of drones with identity-based proxy signcryption," *IEEE Access*, vol. 9, pp. 89133–89142, 2021.

[24] I. Ullah, S. Zeadally, N. U. Amin, M. Asghar Khan, 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, p. 103477, 2021.

[25] 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, article 101692, 2020.

[26] N. W. Lo and J. L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2016.

[27] S. Wang and N. Yao, "LIAP: a local identity-based anonymous message authentication protocol in VANETs," *Computer Communications*, vol. 112, pp. 154–164, 2017.

[28] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

[29] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for VANET," *International Journal of Network Security*, vol. 16, no. 5, pp. 351–358, 2014.