



Yun, C., [Shawky, M. A.](#) and [Ansari, S.](#) (2023) An Optimized Digital Signature Algorithm for Efficient and Secure Authentication in VANETs. In: International Telecommunications Conference (ITC-Egypt'2023), Alexandria, Egypt, 18-20 July 2023, ISBN 9798350326062 (doi: [10.1109/ITC-Egypt58155.2023.10206284](https://doi.org/10.1109/ITC-Egypt58155.2023.10206284))



There may be differences between this version and the published version.
You are advised to consult the published version if you wish to cite from it.

<https://eprints.gla.ac.uk/298665/>

Deposited on 19 May 2023

Enlighten – Research publications by members of the University of Glasgow
<http://eprints.gla.ac.uk>

An Optimized Digital Signature Algorithm for Efficient and Secure Authentication in VANETs

Chenyi Yun[†], Mahmoud A. Shawky[†] , Shuja Ansari[†] 

[†]James Watt School of Engineering, University of Glasgow, Glasgow, G12 8QQ, United Kingdom
Email: 2510937y@student.gla.ac.uk, m.shawky.1@research.gla.ac.uk, Shuja.Ansari@glasgow.ac.uk

Abstract—Vehicular ad-hoc networks (VANETs) are a vital technology for intelligent transportation systems. However, to ensure the security and reliability of VANET applications, it is imperative to implement an effective authentication scheme that can resist different adversarial attacks. This research paper demonstrates the susceptibility of the enhanced Ong, Schnorr, and Shamir (OSS) digital signature scheme proposed by Shawky et al. to replay and impersonation attacks. Then, we propose an efficient authentication scheme that uses the public key infrastructure for initial authentication while pseudo identities are used for message verification. In addition, we propose an improved digital signature scheme that effectively defends against active attacks in vehicular communication. We demonstrate the practicality of the proposed method by implementing it using the Labview platform and discussing its computation cost. Our findings underscore the superiority of the proposed scheme in reducing the computational time required for signature verification in comparison to other existing methods.

Index Terms—Active attacks, Digital signatures, Labview, OSS signatures, Vehicular ad-hoc networks.

I. INTRODUCTION

The adoption of vehicular communication has gained significant momentum in recent years, with applications ranging from road safety to traffic efficiency. One of the principal challenges encountered in securing vehicular ad-hoc networks (VANETs) pertains to preventing active attacks such as impersonation, modification, and replay [1]. In this regard, authentication serves as a crucial security service for addressing these threats. Authentication can typically be categorized into identity and message authentication. While the former involves verifying the legitimacy of the sender's entity by verifying its identity, the latter entails validating the integrity of each received message. This paper focuses on both types of authentication in VANETs, ensuring that only authorized users can participate and communicate with the network.

In the context of VANET, there are three main entities that play crucial roles in ensuring the proper functioning and security of the network. These entities include the trusted authority (TA), roadside units (RSUs), and vehicles' onboard units (OBUs) [2]. The TA serves as a trusted central entity responsible for managing the security and privacy aspects of the network, while the RSUs are stationary units deployed alongside the roads to provide communication and connectivity services to the vehicles. On the other hand, the OBUs are the communication devices installed within vehicles, which

enable them to communicate with other vehicles and RSUs within the network.

In the realm of cryptography-based authentication, there exist three commonly used methods: public key infrastructure (PKI)-based, identity (ID)-based, and group signature (GS)-based authentication [5]. PKI-based methods employ digital signatures to demonstrate that a particular public key belongs to a specific user in the network. Nonetheless, the task of signing and disseminating these certificates among all network terminals falls upon the TA, resulting in a substantial computational and communication overhead. Additionally, the distribution of the certificate revocation list (CRL) among vehicles is associated with high communication costs. In ID-based methods, a user's identity information is utilized to derive the public key, while the key generation center (i.e., TA) computes and distributes the private key based on the provided identity information. This enables the receiver to verify messages using the sender's public key while signing them using their own private key. However, these methods entail significant computational overheads, thereby presenting a challenge [3]. In GS-based methods, the group consists of a manager and members, with each member signing the message on behalf of the group to generate the signature using the sender's secret key, thus offering privacy preservation [4]. Meanwhile, the recipient verifies the received signatures using the group public key. Nevertheless, supporting forward and backward secrecy necessitates reconstructing the entire group for every vehicle joining or leaving the group region, which poses a challenge, especially in high-speed terminals.

In this challenging scenario, Shawky et al. [6] presented a challenge-response identity authentication mechanism that utilizes the elliptic curve cryptosystem (ECC) in combination with the Ong, Schnorr, and Shamir (OSS) digital signatures, in an attempt to design an effective and secure digital signature solution. Unfortunately, this mechanism is susceptible to impersonation and replay attacks. To overcome these vulnerabilities, this paper proposes an enhanced identity authentication mechanism that is capable of resisting such attacks. The following are the main contributions of this paper.

- We prove that the OSS-based digital signature scheme presented by Shawky et al. [6] cannot resist impersonation and replay attacks.
- Then, we propose an effective authentication scheme

that employs an improved OSS-based digital signature algorithm, proving its capability of resisting both active and passive attacks.

- Finally, we evaluate the efficacy of our proposed scheme by implementing it using Labview and evaluating its computational complexities.

This paper is structured as follows. Section II provides a review of authentication methods in VANETs. In Section III, we outline the security issues, problem deviations, and system modeling. Section IV presents our proposed authentication scheme, while Section V presents the simulation results and evaluates the computational complexity of the proposed scheme. Finally, in Section VI, we conclude this work.

II. RELATED WORKS

In the realm of VANETs, the use of cryptography-based authentication schemes has become increasingly common. This section presents a review of various authentication schemes proposed by different researchers in recent years. Liu et al. [7] introduced the first proxy-based authentication scheme, which uses proxy vehicles to verify signatures in support of RSUs and broadcast the verification results. However, this scheme is limited to V2I communication and did not consider V2V communication. Asaar et al. [8] pointed out that the scheme in [7] is vulnerable to impersonation and modification attacks and proposed an improved proxy-based scheme with better computational performance. In this scheme, a number of received signatures are distributed between proxy vehicles for verification. Bayat et al. [9] developed an ID-based scheme that supports batch verification and stores a dynamically updated master key into RSUs' tamper-proof devices (TPDs). Al-shareeda et al. [10] designed a free pairing conditional privacy-preserving authentication scheme, while Lo et al. [11] proposed a solution to address the high computational overhead of bilinear pairing operations. Wei et al. [12] developed a lightweight ID-based solution employing the factorization problem of the RSA cryptosystem for identity verification. However, this scheme was later found to be vulnerable to common modulus attacks by Zhang et al. [13].

Reference [14] proposed a technique based on edge computing where the RSUs verify messages from adjacent vehicles and broadcast the verification results to surrounding vehicles. However, this approach had security weaknesses related to impersonation attacks as demonstrated by Limbasiya et al. [15]. Lyu et al. [16] employed the timed efficient stream loss-tolerant authentication (TESLA) method and elliptic curve-based digital signatures to design a scheme that forecasts the vehicle's future position for immediate message authentication. Zhong et al. [17] implemented a certificateless aggregation signature scheme to reduce the cost of communication and maintain privacy, but neglected to consider V2V applications. Cui et al. [18] developed an elliptic curve cryptosystem ECC-based content-sharing scheme tailored for 5G-enabled vehicular networks, enabling vehicles to efficiently filter their nearby vehicles to select competent and suitable proxy vehicles for content services. Various conditional privacy-preserving

authentication (CPPA) schemes have been proposed in [19]–[25], employing ECC-based scalar multiplication and addition operations. In [20], a pseudo-ID-based scheme is proposed, in which pseudo-identities are exchanged between terminals to offer conditional privacy. By adopting these schemes, vehicles are not required to store any certificates for authentication, and the TA is relieved of the need to retrieve the real identity of malicious vehicles from certificates. In contrast to the works discussed, the proposed authentication scheme integrates the OSS into the ECC for generating digital signatures, providing a secure and efficient approach for initial identity authentication.

III. PROBLEM DEFINITION AND SYSTEM MODELLING

This section defines typical security attacks, evaluates the scheme proposed in [6], and highlights its security vulnerabilities. Finally, a detailed system model is presented.

A. Security Definitions

Digital signature schemes can be vulnerable to various types of attacks, including modification, replay, and impersonation attacks. The following provides detailed definitions of these attacks.

- 1) *Modification attacks*: This attack involves malicious attempts to alter either the signed message or the signature itself, with the goal of changing the message's authenticity or the signer's identity.
- 2) *Replay attacks*: In this attack, the attacker intercepts a signed message and retransmits it to either the original recipient or another recipient with the intention of deceiving them into performing a specific action or revealing sensitive information.
- 3) *Impersonation attacks*: In this attack, the attacker may use stolen or compromised digital certificates or private keys to sign fraudulent messages or transactions.

These attacks highlight the need for robust security measures to be implemented in digital signature schemes, particularly those that are intended for use in critical applications.

B. An Overview and problem definition in [6]

Shawky et al. [6] introduced a novel digital signature scheme that combines the ECC and the OSS digital signature scheme. This hybrid scheme involves a signer and a verifier, where the verifier initiates a communication session by sending a communicating message m to the signer. The signer then generates an invertible 4×4 matrix r , and computes the digital signature x and y using the equations $x = (r + mr^{-1}) \cdot 2^{-1} \pmod{n}$ and $y = (r - mr^{-1}) \cdot 2^{-1} \cdot u^{-1} \pmod{n}$, respectively. The signer then responds to the communication request by sending the digital signatures x and y to the verifier. The verifier, in turn, verifies the received signature using the formula $x^2 + ky^2 = m \pmod{n}$ based on the principles of the OSS scheme, to compute m' . If m' is equal to the original message m , the digital signature is considered verified.

Problem definition: The digital signature scheme presented in [6] has been found to be vulnerable to impersonation attacks. These attacks can take two forms: (1) the attacker can

impersonate the verifier by sending a communication request m , or (2) the attacker can impersonate the signer. In the first case, the attacker can successfully impersonate the verifier since there is no identifiable information to prove that the signer is communicating with the legitimate verifier. In the second case, the attacker eavesdrops on previously transmitted messages $M : [m_1, m_2, \dots, m_n]$ and their associated digital signatures $DS : [(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)]$ generated by different users $U : [U_1, U_2, \dots, U_n]$ and constructs a table T_{Eve} that contains the list of previously transmitted messages M and their associated digital signatures DS . The attacker can then impersonate the i^{th} user $U_i \in U$ if he receives the message $m_i \in M$. In this case, the attacker looks for m_i in the table T_{Eve} , obtains the signature (x_i, y_i) , and transmits it to the verifier, thereby successfully impersonating the i^{th} user. This highlights a significant weakness in the scheme's ability to resist impersonation attacks.

C. System Modelling

The following entities constitute the network architecture of the proposed scheme, see Fig. 1.

- *The trusted authority (TA):* The trusted authority is a trusted entity responsible for managing and issuing digital certificates to vehicles in VANETs.
- *The roadside unit (RSU):* The RSU is a stationary device deployed on the side of the road that facilitates communication between vehicles and the infrastructure.
- *Vehicles' onboard units (OBUs):* The OBU is a wireless communication device installed in vehicles that enables communication with other OBUs and RSUs.
- *The attacker (Eve):* The attacker is an unauthorized entity that attempts to disrupt or exploit the communication and security of a VANET.

IV. THE PROPOSED SCHEME

This section discusses the proposed authentication scheme and explains the signature generation and verification process.

A. The proposed authentication scheme

The proposed authentication scheme employs PKI-based authentication to enable mutual identity verification and establish a symmetric shared key between authorized parties. This scheme is composed of four distinct phases: initialization, registration, initial legitimacy detection, and message signing and verification. Each phase is described in detail as follows.

- 1) *Initialisation phase:* During this phase, the TA generates the public parameters (PPs) for the system. For a security level of 80 bits, the proposed scheme employs the elliptic curve (EC) "secp160k1" with the recommended parameters specified in [26].
- 2) *Registration phase:* During this phase, the TA is responsible for registering the network terminals before joining the network. This phase involves the following steps.
 - *Step 1:* For vehicle (A) registration, the TA chooses A 's private key SC_A and computes its relevant public key PK_A . Then, the TA generates the A 's long-term digital certificate $Cert_A = \langle PK_A, T_R, \sigma_{TA} \rangle$,

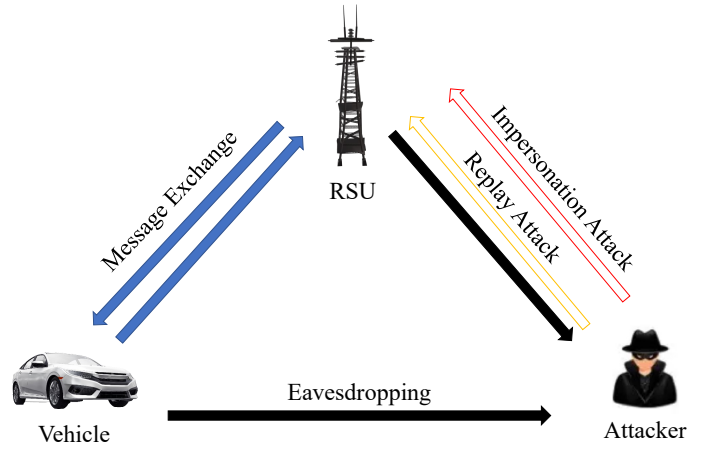


Fig. 1: System modelling.

where T_R is the certificate validation period and σ_{TA} is the TA's signature. Finally, the TA stores $\{PPs, SC_A, Cert_A\}$ into the vehicle's OBU.

- *Step 2:* Similarly, for each RSU (B) registration, the TA chooses B 's private key SC_B , computes its relevant public key PK_B , and generate its certificate $Cert_B = \langle PK_B, T_R, \sigma_{TA} \rangle$. At last, the TA stores $\{PPs, SC_B, Cert_B\}$ into the RSU.
- *Step 3:* The TA distributes the CRL of revoked vehicles, where the CRL comprises the issued certificates of revoked vehicles.

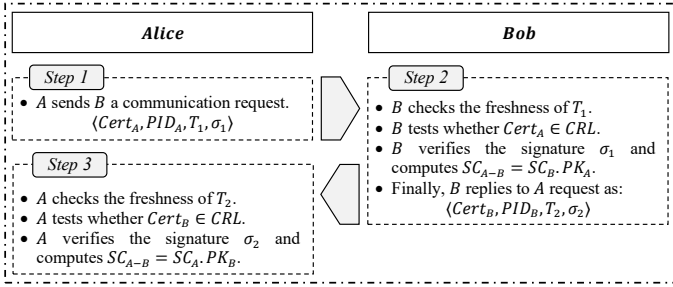
- 3) *Initial legitimacy detection phase:* Let us consider a scenario in which A wants to establish secure communication with B within range. This phase involves the following steps.

- *Step 1:* In this step, A sends B a communication request in the form of $\langle Cert_A, PID_A, T_1, \sigma_1 \rangle$, where T_1 is the timestamp of the generated signature $\sigma_1 = Sign_{SC_A}(Cert_A || PID_A || T_1)$.
- *Step 2:* B checks the freshness of the received timestamp T_1 , finds out if $Cert_A \in CRL$, and verifies σ_1 . Then, B replies by sending the tuple $\langle Cert_B, PID_B, T_2, \sigma_2 \rangle$ to A , where $\sigma_2 = Sign_{SC_B}(Cert_B || PID_B || T_2)$.
- *Step 3:* A , in turn, checks the freshness of the received timestamp T_2 , finds out if $Cert_B \in CRL$, and verifies σ_2 .
- Finally, both terminal agrees on a symmetric shared key SC_{A-B} computed as $SC_{A-B} = SC_A.PK_B$ and $SC_{A-B} = SC_B.PK_A$ at the sides of Alice and Bob, respectively, using Diffie-Hellman key exchanging protocol.

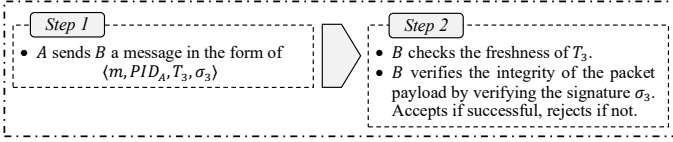
Fig. 2(a) shows the description flowchart of this phase.

- 4) *Message signing and verification phase:* In this phase, A sends a safety-related message m containing information about the vehicle's location, heading, and speed. The following steps describe this phase.

- *Step 1:* In this step, A sends B the message m



(a) Description diagram of the initial legitimacy detection phase.



(b) Description diagram of the message signing and verification phase.

Fig. 2: A Schematic diagram of the initial legitimacy detection and message signing and verification Phases.

in the form of $\langle m, PID_A, T_3, \sigma_3 \rangle$, where $\sigma_3 = \text{Sign}_{SC_{A-B}}(m || PID_A || T_3)$

- *Step 2:* *A*, in turn, checks the freshness of the received timestamp T_3 and verifies σ_3 .

Fig. 2(b) shows the description flowchart of this phase.

It should be noted that the signatures $\{\sigma_1, \sigma_2\}$ have been generated using the traditional *EC* digital signature algorithm while the proposed digital signature algorithm outlined in the following subsection has been utilized to generate σ_3 .

B. The proposed digital signature algorithm

This subsection presents an improvement to the digital signature algorithm of Shawky et al. [6]. To generate a valid signature $\sigma_3 = \text{Sign}_{SC_{A-B}}(m || PID_A || T_3)$ of the packet payload $\langle m, PID_A, T_3 \rangle$. In this context, the signature generation stage comprises the following steps.

- *Step 1:* Using the symmetric shared key SC_{A-B} , *A* generates the 4×4 self-invertible matrix r formulated as follows.

$$r = \begin{bmatrix} K_A & K_B \\ K_C & K_D \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{bmatrix} \quad (1)$$

where $K_B = I - K_A$, $K_C = I + K_A$, $K_A + K_D = 0$, and I is the identity matrix. Accordingly, the first and second rows in the K_A matrix is given by $\{SC_{A-B}\}_x \cdot \mathbb{G} = (K_{11}, K_{12})$ and $\{SC_{A-B}\}_y \cdot \mathbb{G} = (K_{21}, K_{22})$, respectively, where $\{\}_x$ and $\{\}_y$ denote the x and y coordinates of the *EC* point SC_{A-B} and \mathbb{G} is the base point.

- *Step 2:* In this step, *A* generates the signature of the hashed value of the packet payload $h = \text{Hash}(m || PID_A || T_3)$ using the following formula.

$$\begin{aligned} x &\equiv (r + hr^{-1}) \cdot 2^{-1} \pmod{n} \\ y &\equiv (r - hr^{-1}) \cdot 2^{-1} \cdot u^{-1} \pmod{n} \end{aligned} \quad (2)$$

where $u = SC_A$ is *A*'s private key and n is the RSA moduli [6]. Finally, $\{x, y, k\}$ represents the signature σ_3 , where k is a public parameter transmitted as a part of the signature and equals $-u^2 \pmod{n}$.

For signature verification, *B* computes $h = \text{Hash}(m || PID_A || T_3)$. Then, *B* uses the received signature σ_3 to compute h' as follows.

$$h' = x^2 + ky^2 \pmod{n} \quad (3)$$

Finally, *B* verifies the σ_3 by testing whether $h = h'$ happens or not. The following presents the proof of correction of (3).

$$\begin{aligned} x^2 + ky^2 &\equiv ((r + hr^{-1}) \cdot 2^{-1})^2 \\ &\quad + (-u^2) \cdot ((r - hr^{-1}) \cdot 2^{-1} \cdot u^{-1})^2 \\ &\equiv 2^{-2} [(r^2 + h'^2 r^{-2} + 2hr') \\ &\quad - (u^2 \cdot u^{-2}) (r^2 + h'^2 r^{-2} - 2hr')] \\ &\equiv 2^{-2} (2hr' + 2hr') \equiv h' \pmod{n} \end{aligned} \quad (4)$$

Fig. 3 presents the description flowchart for the proposed digital signature algorithm.

V. PERFORMANCE EVALUATION

This section discusses the security strength and the computation complexity of the proposed scheme.

A. Security analysis

This subsection discusses the scheme's security strength against typical attacks.

- *Resistance to impersonation:* This attack targets the initial legitimacy detection phase or the message signing and verification phase, with the objective of impersonating either party *A* or *B*. The attack takes two distinct forms: (1) impersonating a legitimate terminal, and (2) generating a valid signature. In the first case, the attacker's ability to impersonate legitimate terminals is limited by the difficulty of solving the discrete logarithm problem, as they lack knowledge of the users' private keys. In the second case, the attacker is hindered by the difficulty of solving the factorization problem, which makes generating a valid signature a challenging task.
- *Resistance to replay:* In the context of this attack, replaying a previously transmitted message is difficult for the attacker, as the recipient employs a freshness-checking mechanism that examines the attached timestamp of each received signature. This mechanism effectively thwarts replay attacks.
- *Resistance to modification:* In this particular attack, Eve aims to modify the message contents and resend it to the targeted terminal. However, the recipient implements an integrity verification mechanism that scrutinizes the attached signatures. These signatures are challenging to forge, given the difficulty associated with solving the discrete logarithm problem and factorization problem in the initial legitimacy detection phase and message signing and verification phase, respectively.

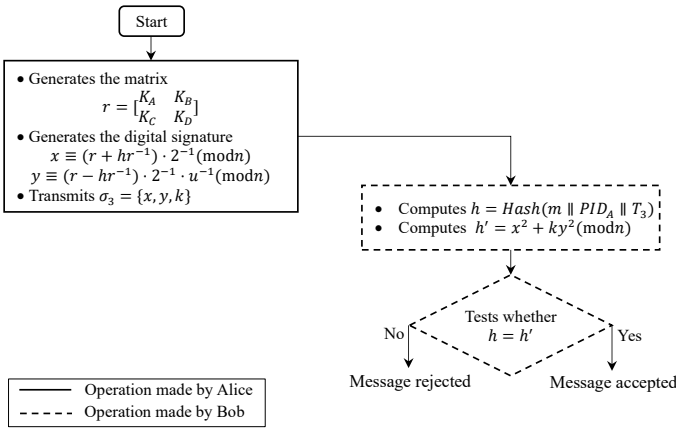


Fig. 3: Description flowchart for the proposed digital signature algorithm.

B. Simulation analysis and computation comparison

The authentication scheme’s effectiveness is gauged by the recipient’s ability to validate multiple safety-related messages, enabling communication with a large number of vehicles concurrently and enhancing network scalability. The proposed digital signature algorithm offers a crucial advantage in that the computational complexity associated with verifying received messages utilizing (3) is exceptionally low, taking only a few microseconds. By contrast, conventional elliptic curve digital signature algorithms can cost several milliseconds, making this algorithm an attractive option for efficient message verification. In this context, Table I presents the computational time for calculating different cryptographic operations measured using the Labview platform and an Intel(R) Core(TM) *i7 – 10850H* CPU running at a clock speed of *2.70GHz* and backed by *16 GB* of RAM.

Table II displays the computational time necessary to sign a single message and verify a quantity of n received signatures using the proposed scheme, in comparison to the approach outlined in [21], [22]. Our analysis reveals that the proposed scheme incurs a higher computation cost than that of [21], [22], although this elevated expense remains within an acceptable range given that each vehicle transmits a solitary safety-related message every $100–300\text{ msec}$ via the dedicated short-range communication (DSRC) protocol [1]. In terms of signature verification, the proposed scheme proves to be more efficient than the method proposed in [21], [22]. These findings are further illustrated by Fig. 4, which depicts the time required to verify varying numbers of n messages, ranging from 1 to 1000. This data provides compelling evidence of the proposed scheme’s superior performance capabilities.

VI. CONCLUSIONS

This research paper proposes an authentication scheme that utilizes PKI-based authentication for initial legitimacy detection and pseudo-identities for message signing and verification. We also demonstrate the vulnerability of the scheme presented

TABLE I: The time cost of various crypto-based operations

Symbol	Definition	Time (msec)
$T_{Eq.(1,2)}^{OSS}$	Time cost of computing equations (1) and (2)	6.135
$T_{Eq.(3)}^{OSS}$	Time cost of computing equation (3)	0.036
T_{Mul}^{ECC}	Time cost of ECC-based point multiplication	1.535
T_{Add}^{ECC}	Time cost of ECC-based point addition	0.705
T_h	Time cost of the SHA-1 hashing operation	0.014

TABLE II: Computation comparison

No.	Signature generation	Signature verification
[21]	$2T_{Mul}^{ECC} + 2T_h \approx 3.098$	$(3n)T_{Mul}^{ECC} + (2n)T_{Add}^{ECC} + (2n)T_h \approx 6.043n$
[22]	$3T_{mul}^{ECC} + 2T_h$ ≈ 4.633	$(2n + 2)T_{mul}^{ECC} + (2n + 1)T_{add}^{ECC} + (3n)T_h$ $\approx 4.522n + 3.775$
Ours	$T_{Eq.(1,2)}^{OSS} + T_h \approx 6.14$	$(n)T_{Eq.(3)}^{OSS} + (n)T_h \approx 0.05n$

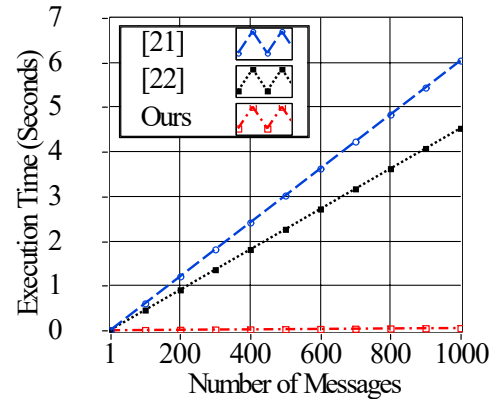


Fig. 4: The time required for verifying different numbers of messages.

in [6] to impersonation attacks, followed by the introduction of an improved digital signature algorithm that incorporates the elliptic curve cryptosystem into the OSS digital signature scheme. The security robustness of the proposed scheme against common attacks has been verified. Furthermore, performance analyses have been successfully conducted through simulations. The results indicate that the proposed scheme can significantly reduce the time required for verifying 1000 messages, achieving a reduction of approximately 99% compared to the approach presented in [21], [22]. As part of our future research, we will explore the feasibility of implementing the proposed authentication scheme in real-time scenarios.

REFERENCES

- [1] A. Shawky, M. Usman, D. Flynn, M. A. Imran, Q. H. Abbasi, S. Ansari, and A. Taha, “Blockchain-based secret key extraction for efficient and secure authentication in VANETs”, *J. Inf. Secur. Appl.*, vol. 74, 103476, 2023.
- [2] S. S. Manvi and S. Tangade, “A Survey on Authentication Schemes in VANETs for Secured Communication”, *Vehicular Communications*, vol. 9, pp. 19-30, Jul. 2017.

- [3] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks", *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422-2433, Jan. 2021.
- [4] M. A. Shawky, M. Usman, M. A. Imran, Q. H. Abbasi, S. Ansari, and A. Taha, "Adaptive chaotic map-based key extraction for efficient cross-layer authentication in VANETs", *Vehicular Communications*, vol. 39, 100547, pp. 2422-2433, Jan. 2023.
- [5] M. A. Shawky, M. Bottarelli, G. Epiphaniou, and P. Karadimas, "An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks", *IEEE Transactions on Vehicular Technology*, doi: 10.1109/TVT.2023.3244077.
- [6] H. M. Elkamchouchi, A. E. Takieldein, and M. A. Shawky, "An advanced hybrid technique for digital signature scheme", in 2018 5th International Conference on Electrical and Electronic Engineering (ICEEE), pp. 375-379, 2018.
- [7] Y. Liu, L. Wang, and H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks", *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3697-3710, Oct. 2014.
- [8] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, "A secure and efficient authentication technique for vehicular ad-hoc networks", *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5409-5423, Jun. 2018.
- [9] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A new and efficient RSU based authentication scheme for VANETs", *Wireless Networks*, vol. 26, pp. 3083-3098, 2019.
- [10] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network", *Symmetry*, vol. 12, no. 10, pp. 1687-1712, Sep. 2020.
- [11] 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, May 2016.
- [12] Z. Wei, J. Li, X. Wang, and C. Gao, "A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing", *IEEE Access*, vol. 7, pp. 62785-62793, 2019.
- [13] G. Zhang, Y. Liao, Y. Fan, and Y. Liang, "Security analysis of an identity-based signature from factorization problem", *IEEE Access*, vol. 8, pp. 23277-23283, 2020.
- [14] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks", *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1621-1632, May 2019.
- [15] T. Limbasiya and D. Das, "Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication", *IEEE Systems*, vol. 14, no. 1, pp. 520-529, Mar. 2020.
- [16] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: Prediction-based authentication for vehicle-to-vehicle communications", *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 71-83, 2016.
- [17] 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.
- [18] J. Cui, J. Chen, H. Zhong, et al., "Reliable and efficient content sharing for 5G-enabled vehicular networks", *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1247-1259, Feb. 2022. doi: 10.1109/TITS.2020.3023797.
- [19] 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.
- [20] J. Li, K. R. Choo, W. Zhang, S. Kumarid, J. J. P. C. Rodrigues, M. K. Khan, and D. Hogrefe, "EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks", *Vehicular Communications*, vol. 13, pp. 40-50, 2018.
- [21] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment", *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5535-5548, 2020.
- [22] Y. Ming and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in VANETs", *Mobile Information Systems*, vol. 2019, p. 7593138, 2019.
- [23] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs", *IEEE Access*, vol. 8, pp. 2482-2498, 2020.
- [24] J. Li, Y. Ji, K.-K. R. Choo, and D. Hogrefe, "CL-CPPA: Certificate-less conditional privacy-preserving authentication protocol for the internet of vehicles", *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10332-10343, 2019.
- [25] Y. Wang, Y. Liu, and Y. Tian, "ISC-CPPA: Improved-Security Certificateless Conditional Privacy-Preserving Authentication Scheme With Revocation", *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 12304-12314, 2022.
- [26] Certicom Research, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters 1.0, pp. 9-10, Sep. 2000.