applied sciences

MDPI

Article

Chebyshev Polynomial-Based Scheme for Resisting Side-Channel Attacks in 5G-Enabled Vehicular Networks

Mahmood A. Al-Shareeda [1], Selvakumar Manickam [1,*], Badiea Abdulkarem Mohammed [2], Zeyad Ghaleb Al-Mekhlafi [2], Amjad Qtaish [2], Abdullah J. Alzahrani [2], Gharbi Alshammari [2], Amer A. Sallam [3] and Khalil Almekhlafi [4]

[1] National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, USM, Penang 11800, Malaysia; m.alshareeda@nav6.usm.my
[2] College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia; b.alshaibani@uoh.edu.sa (B.A.M.); ziadgh2003@hotmail.com (Z.G.A.-M.); am.qtaish@uoh.edu.sa (A.Q.); aj.alzahrani@uoh.edu.sa (A.J.A.); gk.alshammari@uoh.edu.sa (G.A.)
[3] Engineering and Information Technology College, Taiz University, Taiz 6803, Yemen; amer.sallam@taiz.edu.ye
[4] CBA-Yanbu, Taibah University, Al Madinah 42353, Saudi Arabia; drkhalilalmekhlafi@gmail.com
* Correspondence: selva@usm.my; Tel.: +604-653-3004

Abstract: The privacy and security vulnerabilities in fifth-generation (5G)-enabled vehicular networks are often required to cope with schemes based on either bilinear pair cryptography (BPC) or elliptic curve cryptography (ECC). Nevertheless, these schemes suffer from massively inefficient performance related to signing and verifying messages in areas of the high-density traffic stream. Meanwhile, adversaries could launch side-channel attacks to obtain sensitive data protected in a tamper-proof device (TPD) to destroy the system. This paper proposes a Chebyshev polynomial-based scheme for resisting side-channel attacks in 5G-enabled vehicular networks. Our work could achieve both important properties of the Chebyshev polynomial in terms of chaotic and semi-group. Our work consists of five phases: system initialization, enrollment, signing, verification, and pseudonym renew. Moreover, to resist side-channel attacks, our work renews periodically and frequently the vehicle's information in the TPD. Security analysis shows that our work archives the privacy (pseudonym identity and unlikability) and security (authentication, integrity, and traceability) in 5G-enabled vehicular networks. Finally, our work does not employ the BPC or the ECC; its efficiency performance outperforms other existing recent works, making it suitable for use in vehicular networks.

Keywords: Chebyshev polynomial; side-channel attacks; 5G-enabled vehicular networks; semi-group; privacy and security; chaotic map

Citation: Al-Shareeda, M.A. ; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. Chebyshev Polynomial-Based Scheme for Resisting Side-Channel Attacks in 5G-Enabled Vehicular Networks. *Appl. Sci.* **2022**, *12*, 5939. https://doi.org/10.3390/app12125939

Academic Editor: Arcangelo Castiglione

Received: 19 May 2022
Accepted: 8 June 2022
Published: 10 June 2022

1. Introduction

A vehicle is a critical component of a person's ability to complete daily activities. Various scholars have investigated and studied fifth-generation (5G) networks, which can help support passengers and drivers.

As the next deployment of cellular communication, the 5G networks have regained renewed interest in international academia [1–3]. The 5G network has the characteristics of a wide covered area increased by 1000 times, battery life reduced by five times, and high bandwidth improved by 10 Gbps compared to the fourth generation (4G). It brings many new challenges for mobile ad hoc networks (MANET), especially for vehicular networks [4–6].

In vehicular networks, the vehicle communicates with neighboring others, utilizing an equipped onboard unit (OBU) in a public environment through vehicle–vehicle (V2V) communication. By sharing data between vehicles, users can employ instant messages acquired from others to reduce road accidents, provide traffic safety, and avoid road jams [7,8].

Due to the nature of the public environment, vehicular networks are vulnerable to various privacy and security issues. Therefore, many scholars have focused on satisfying privacy and security requirements for vehicular networks by proposing sophisticated authentication schemes. Nevertheless, more precisely, some existing schemes are vulnerable to side-channel attacks to obtain the sensitive information saved on the tamper-proof device (TPD) of the vehicle. Thereby, if the attacker compromises the private key of "trusted authority (TA)" saved of any TPD, the entire system will be insecure and exposed. Furthermore, the existing schemes use more complex and time-consuming operations such as "bilinear pair cryptography" and "elliptic curve cryptography" to sign and verify the messages.

As a result, this paper proposes a Chebyshev polynomial-based scheme for resisting side-channel attacks in 5G-enabled vehicular networks, which could achieve both important properties in terms of chaotic and semi-group. To the best of the author's knowledge, our work is the first Chebyshev polynomial-based scheme for 5G-enabled vehicular networks without using bilinear pair cryptography or elliptic curve cryptography. More precisely, the main contributions of this paper are threefold.

- First, a Chebyshev polynomial-based scheme for resisting side-channel attacks in 5G-enabled vehicular networks that fulfills the design goals with regard to the privacy and security requirements;
- Second, a scheme that resists side-channel attacks by regularly renewing the system's sensitive information (pseudonym) preserved in the TPD;
- Third, a scheme that outperforms other works based on bilinear pair cryptography and elliptic curve cryptography schemes; therefore, it the suitable for large-scale deployment in vehicular networks.

The remainder of this paper is arranged as follows. In Section 2, the previous existing works are reviewed. The architectural design, design goal, threat model, and mathematical foundations are introduced in Section 3. We propose a Chebyshev polynomial-based scheme for secure 5G-enabled vehicular networks in Section 4 and the security analysis of our work in Section 5. Section 6 evaluates the efficiency performance. Ultimately, we conclude the paper in Section 7.

2. Related Work

Recently, both secure authentication and privacy-preserving are the most critical issues for vehicular networks. To address these issues, several scholars have concentrated on satisfying privacy and security requirements for vehicular networks. The three authenticated approaches are introduced separately in the following subsections.

2.1. Public Key Infrastructure (PKI)-Based

The rationale behind PKI-based is primarily to preload many anonymous certifications and the relevant pair of keys (private/public keys) to each enrolled vehicle in advance. Many researchers [9–17] have proposed the PKI-based scheme for satisfying privacy and security in vehicular networks. However, the three main limitations of this approach are (i) huge certification management burden for TA, since massive numbers of anonymous certifications and the relevant pair of keys are required; (ii) storage management burden due to the small storage capacity of the vehicle; and (iii) low efficiency of the system, since the certificate is also verified in the verification method.

2.2. Group Signature (GS)-Based

The rationale behind GS-based is that the group administrator is responsible for generating the signature on the behalf of the whole group or members. Many researchers [18–22] have proposed a GS-based scheme to tackle the vulnerabilities arising from the PKI-based scheme in a vehicular network. However, the two main limitations of this approach are (i) the huge size of the certificate revocation list (CRL) owing to the growing number of

revoked vehicles; and (ii) the low efficiency of the system, since two pairing operations are included.

2.3. Pseudonym-Based

The main motivation behind the pseudonym-based approach is to address the three main limitations and two main limitations arising from the PKI-based and GS-based vehicular networks, respectively. The rationale behind the pseudonym-based approach is that the public key is extracted from the vehicle's identification, and the master key is created by a trusted authority. At present, the two cryptographic methods could use the pseudonym-based approach. The following methods for this approach are introduced separately.

- Bilinear Pair Cryptography (BPC):
  In 2008, Zhang et al. [23] were the first to propose the bilinear pair cryptography and pseudonym-based approach to achieve security communication in vehicular networks. The scheme of Zhang et al. [23] stores the secret key of the system (TA) in the TPD of the vehicle, which is claimed not to be compromised by the adversary.
  In 2013, Lee and Lai [24] highlighted the limitation arising from the scheme of Zhang et al. [23]: it could not achieve non-repudiation and replay attacks resistance. Therefore, Lee and Lai [24] proposed an enhanced scheme to satisfy privacy preservation in vehicular networks.
  Later, Bayat et al. [25], and Jianhong et al. [26] highlighted the limitation arising from the scheme of Lee and Lai [24]: it could not resist the impersonation attacks in 2015 and 2014, respectively.
  In 2016, Lei Zhang et al. [27] designed a pseudonym-based authentication scheme to resist side-channel attacks by periodically renewing the sensitive data preserved on the TPD of the vehicle.
- Elliptic Curve Cryptography (ECC):
  In 2015, He et al. [28] were the first to propose the use of elliptic curve cryptography rather than bilinear pair cryptography to achieve privacy and security requirements in vehicular networks. He et al. [28] also highlighted the limitation arising from the schemes of Lee and Lai [24] and Jianhong et al. [26]: they could not resist forgery attacks. However, due to the secret key of the system (TA) being saved on the TPD, the scheme of He et al. [28] suffers from side-channel attacks to retrieve the data for impersonating legal vehicles and sending fake messages in the vehicular networks. In 2017, Wu et al. [29] designed a pseudonym-based scheme in which TA preloaded a batch of pseudonym identities for each enrolled vehicle to provide secure communication in vehicular networks. In 2020, Cui et al. [30] presented a mutual authentication with privacy preservation to resist side-channel attacks by using operation ECC. In 2020, the TA in the scheme of Cui et al. [31] preserved the secret key to the TPD of OBU for enrolled vehicles. In 2019, the scheme proposed by [32] employs time-consuming operations with regards to scalar multiplication-based ECC to check several messages in the urban area.

In order to address the aforesaid issues existing in vehicular networks, this paper will propose the Chebyshev polynomial-based scheme for resisting side-channel attacks in 5G-enabled vehicular networks. Our work will regularly renew the sensitive data preserved in the TPD of the vehicle by using Chebyshev polynomial operations rather than a bilinear pair or ECC. Due to bilinear pairs or ECC not being utilized, our work has high efficiency; thereby, the computation and communication cost compared to other related schemes is lower.

3. Preliminaries

In this section, the preliminaries of our work are introduced in detail in the following subsection.

3.1. Architectural Design

As shown in Figure 1, the architectural design of our work for 5G-enabled vehicular networks is as follows.

- TA: Fully trusted component for vehicular networks. It is responsible for generating Chebyshev polynomial-based public parameters of the system and preloading them into enrolled vehicles.
- 5G-BS: Base station device installed on the roadside. It is responsible for tossing the messages from vehicles to TA or vice versa.
- OBU: Each vehicle has an onboard unit (OBU) to process, send and receive messages. Each OBU has a TPD to preserve sensitive data.

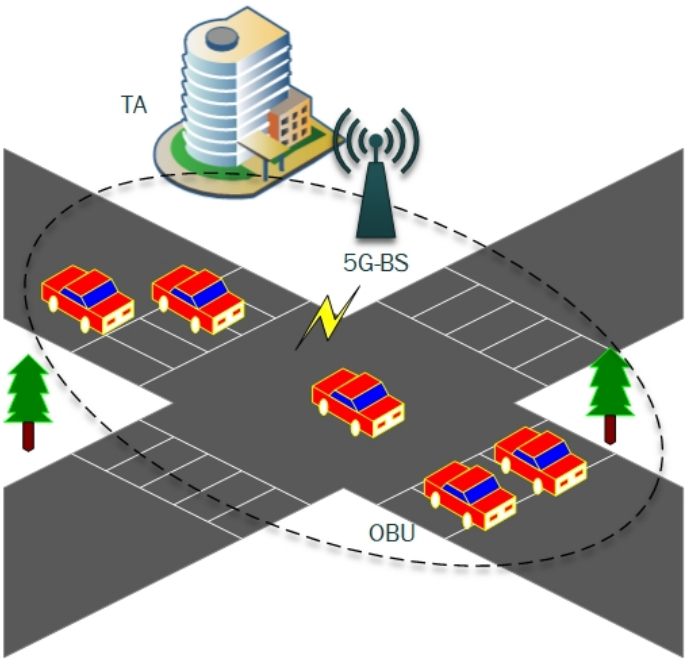


Figure 1. Architectural design of our work for 5G-enabled vehicular networks.

3.2. Design Goal

Our work should achieve the following design goals:

- Pseudonym Identity: The adversary is not capable of disclosing the original identity of the vehicle from the information sent from any enrolled user.
- Authentication and Integrity: Each piece of information sent by a vehicle is checked by enrolled vehicles. Furthermore, enrolled vehicles should be capable of detecting any alteration of received messages.
- Traceability: The TA is the only component capable of revealing the original identity of the vehicle in case it is needed.
- Unlinkability: The adversary is not capable of tracking the behavior of the vehicle by linking two messages sent from the same source.
- Resistance Security Attacks: The sophisticated schemes should resist security attacks again, as will be explained in the coming subsection.

3.3. Threat Model

Our work should resist the threat model.

- Side-Channel Attack: The adversary may retrieve the sensitive information saved on the TPD of the vehicle in order to realize his/her workable advantage.
- Replay Attack: The adversary may replay the previous message sent by the enrolled vehicle in order to realize his/her workable advantage.

- Modify Attack: The adversary may modify the message sent by the enrolled vehicle in order to realize his/her workable advantage.
- Forgery Attack: The adversary may impersonate the enrolled vehicle in order to realize his/her workable advantage.
- Man-In-The-Middle Attack: The third party may intercept the communication among enrolled vehicles in order to realize his/her workable advantage.

3.4. Mathematical Foundations

This subsection describes in detail the concept of Chebyshev polynomial mapping and its two hard assumption problems that are used in our work.

- Chebyshev polynomial:

  Definition 1. *Assume n and P indicate an integer and a large prime number, respectively. x indicates a variable taking values over the interval* $[-\infty, \infty]$. $\mathcal{T}_n(.)$*: a Chebyshev polynomial* $[-\infty, \infty] \rightarrow [-\infty, \infty]$ *of stage n is identified as*

$$\mathcal{T}_n(x) = cos(n * arccos(x)) \tag{1}$$

  Thereby, based on **Definition 1**, the recurrence formulation of the Chebyshev polynomial mapping $\mathcal{T}_n : R \rightarrow R$ is as below:

$$\mathcal{T}_n(x) \equiv 2x\mathcal{T}_{n-1}(x) - \mathcal{T}_{n-2}(x)(modP), (n \geqslant 2) \tag{2}$$

  where $\mathcal{T}_0(x) = 1$ and $\mathcal{T}_1(x) = x$. In addition, some examples of the Chebyshev polynomial are

$$\begin{aligned} \mathcal{T}_2(x) &= 2x^2 - 1, \\ \mathcal{T}_3(x) &= 4x^3 - 3x, \\ \mathcal{T}_4(x) &= 8x^4 - 8x^2 + 1 \end{aligned}$$

  The Chebyshev polynomial has two significant properties, namely chaotic and semi-group, respectively.
  - Chaotic property: When degree n > 1, it can identify a Chebyshev polynomial mapping as a chaotic mapping $\mathcal{T}_w : [-\infty, \infty] \rightarrow [-\infty, \infty]$ with a constant density function $f^*(y) = 1/(\pi\sqrt{1-y^2})$.
  - Semi-group property:

$$\begin{aligned} \mathcal{T}_w(\mathcal{T}_l(x)) &= cos(wcos^{-1}(cos(lcos^{-1}(x)))) \\ &= cos(wlcos^{-1}(x)) \\ &= \mathcal{T}_{wl}(x) \\ &= \mathcal{T}_l(\mathcal{T}_w(x)) \end{aligned}$$

    where l and w are integers of positive as well as $x \in [-\infty, \infty]$

  The two hard assumption problems are introduced.

Definition 2. *"Chebyshev polynomial-based Diffie–Hellman problem (CPDHP)": The main task of CPDHP is to estimate the* $\mathcal{T}_{wl}(x)$ *for three given parts* $\mathcal{T}_w(x)$, $\mathcal{T}_l(x)$ *and* x.

Definition 3. *"Chebyshev polynomial-based Discrete Logarithm problem (CPDLP)": The main work of CPDLP is to find the unknown value w such that* $\mathcal{T}_w(x) \equiv y$ *for two given parts x and y.*

4. Proposed Scheme

To prevent the security attacks such as side-channel attacks etc, this paper proposes a secure data-sharing scheme for 5G-enabled vehicular networks. Our work employs Chebyshev polynomial operations rather than more complex operations such as bilinear pair and ECC to renew the sensitive information stored on the OBU of the vehicle. Our work for 5G-enabled vehicular networks consists of five phases: System Initialization, Enrollment, Signing, Verification, and Pseudonym Renew. Figure 2 presents the architecture of our work phases. The TA is in charge of issuing the system parameters based on the Chebyshev polynomial. During the enrollment phase, these parameters are preloaded on each registered vehicle in advance before leaving the factory. After the enrolled vehicle is received, it measures its signature of messages, and the receiver will verify these signatures. When the attacker launches a side-channel attack that causes some damage, the TA should have the capability to renew the pseudonym of the vehicle through 5G-BS securely. Table 1 tabulates the notations and definitions used in these phases of our work.

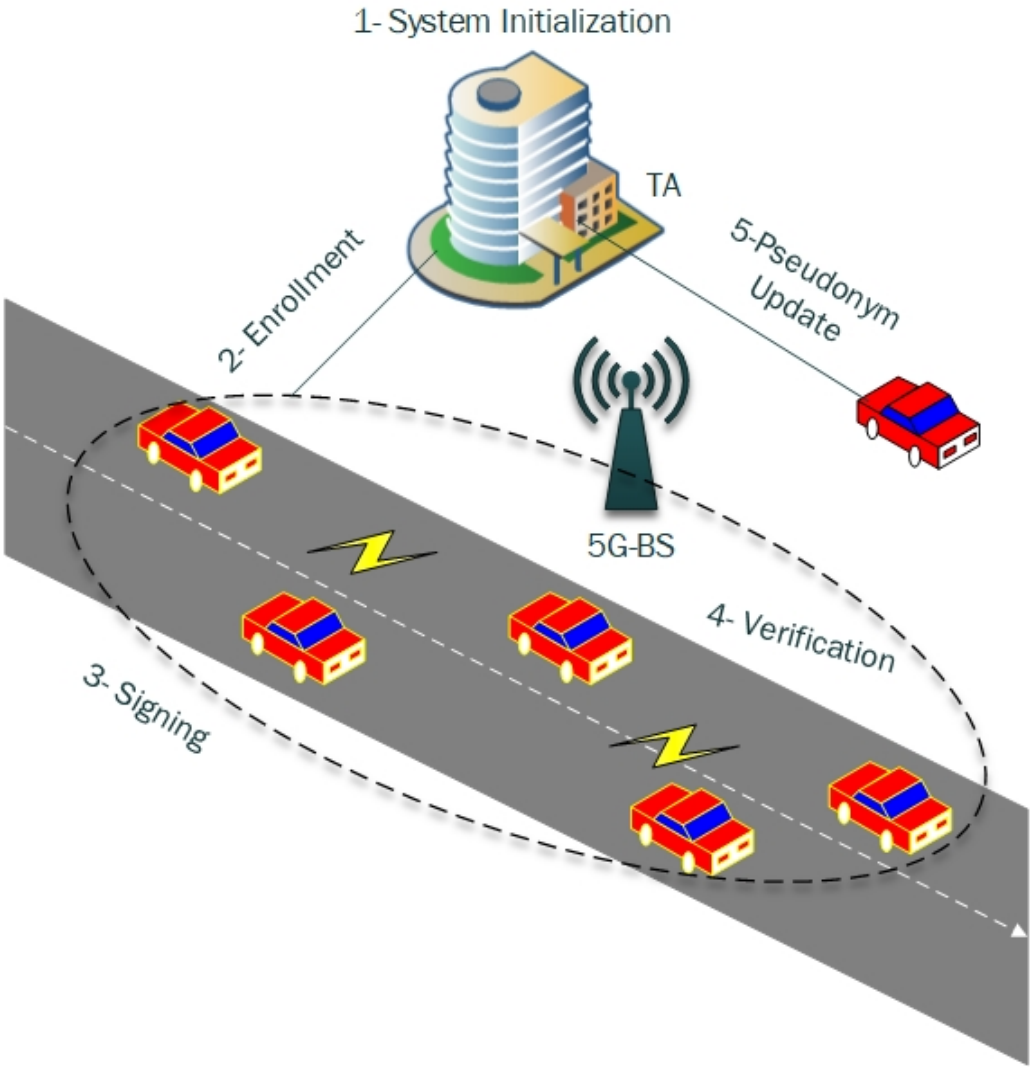


Figure 2. Our work scheme phases.

Table 1. Notations and Definitions Used.

Notations	Definition
TA	The trusted authority
5G-BS	The 5G-base station
OBU	The onboard unit
TPD	The tamper-proof device
ψ	The system parameters
P	A large prime
OID_{v_i}	The original identity of vehicle V_i
h	The hash function based on the chaotic map
SVP_{v_i}	A short valid period
$IPID_{v_i}$	An inter-pseudonym identity
T_r	The time of arriving
$T_\bigtriangledown$	The time of predefined delay
T_{v_i}	The current timestamp
$\vert\vert$	The concatenation operation
$\oplus$	The exclusive-OR operation

4.1. System Initialization

Before the deployment of 5G-enabled vehicular networks, the TA issues system parameters through each of the following steps in the system initialization phase.

- The TA chooses the large prime P and generates values k_s, x based on chaotic map.
- The TA picks a random values s as its secret key.
- The TA determines one hash function h based on the chaotic map, where $h : [-0, 1]^* \rightarrow [-0, 1]^l$.
- The TA publishes the parameters of system $\psi = \{ k_s, x, P, h\}$.

4.2. Enrollment

Before the user leaves the factory in 5G-enabled vehicular networks, the vehicle needs to execute the enrollment process with the system (TA) through the secure channel as follows.

- The user sends the vehicle's original identity OID_{v_i} to the TA.
- The TA first tests the legitimacy of OID_{v_i}; if it is true, the TA continues with the subsequent steps; otherwise, it stops.
- The TA chooses a short valid period SVP_{v_i}, such as 1 January 2022–1 February 2022.
- The TA computes $A_{v_i} = h(s||ev_i)$ and inter-pseudonym identity $IPID_{v_i} = h(OID_{v_i}||A_{v_i}||SVP_{v_i})$.
- The TA preloads the tuples $\{\psi, A_{v_i}, SVP_{v_i}, IPID_{v_i}\}$ to the vehicle. At the same time, it put the tuples into the list of members of the TA.
- The vehicle stores the tuples into TPD.

Note that sensitive data are stored in TPD, which could be disclosed by a third party when these data are still saved for a long time. Thereby, the adversary can successfully launch a side-channel attack to retrieve the data for impersonating a legal vehicle and sending fake messages.

4.3. Signing

Before the messages are exchanged in 5G-enabled vehicular networks, the enrolled vehicle V_i needs to sign the messages with its private key as below. Figure 3 explains the process of the signing phase in detail.

- The vehicle V_i randomly picks a value w and computes public pseudonym identity $PPID_{v_i} = IPID_{v_i} \oplus h(A_{v_i}||T_{v_i})$, where T_{v_i} is the latest timestamp.
- The vehicle calculates the parameter $Pr_{vi} = \mathcal{T}_{PPID_{vi}.w}(x) mod P$.
- The vehicle signs the message $SM_{vi} = h(M_i||PPID_{vi}||T_{vi})$.

- The vehicle calculates the message signature $\sigma_{vi} = \mathcal{T}_{SM_{vi}}(Pr_{vi}) mod P$.
- Lastly, the vehicle broadcasts the message-tuple $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ to others.

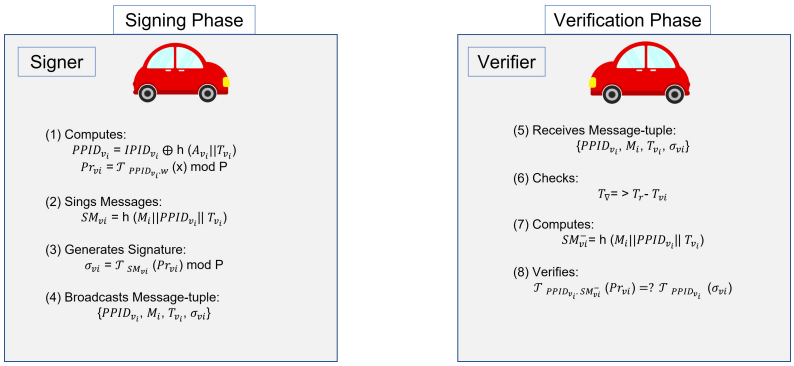


Figure 3. Signing and verification phases.

4.4. Verification

Before accepting the message M_i for further processing, the receiver-enrolled vehicle needs to test whether the message-tuple $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ is valid or not. As well, Figure 3 explains the process of the verification phase in detail.

- When the message-tuple arrives $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$, the receiver v_j initially tests the freshness of timestamp T_{vi} as follows. Assume T_r is the time of arriving and T_∇ is the time of predefined delay. If $(T_\nabla > T_r - T_{vi})$, thereafter T_{vi} is legitimate. Otherwise, the message-tuple $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ is discarded.
- Then, the receiver computes the parameter $SM_{vi}^{-} = h(M_i||PPID_{vi}||T_{vi})$.
- Lastly, the receiver utilizes the message signature σ_{vi} of the message-tuple $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ to verify the message M_i, where $\sigma_{vi} = \mathcal{T}_{SM_{vi}}(Pr_{vi}) modP$. The receiver accepts the tuple when the following equation holds. Otherwise, the message is rejected.

$$\mathcal{T}_{PPID_{v_i}.SM_{vi}^{-}}(Pr_{vi}) \stackrel{?}{=} \mathcal{T}_{PPID_{v_i}}(\sigma_{vi}) \tag{3}$$

4.5. Pseudonym Renew

This phase indicates the main effect of the proposed scheme, which is renewing the pseudonym identity of the vehicle before the attacker could destroy the 5G-enabled vehicular networks by launching side-channel attacks. This phase is as follows. Before the short valid period, SVP_{v_i} is to expire; the registered vehicle needs to renew the inter-pseudonym identity $IPID$ saved on its TPD through 5G-BS to resist side-channel attacks. Once this phase waits for many years, the attacker has enough time to disclose data saved for impersonating legal vehicles and sending fake messages in 5G-enabled vehicular networks. The following steps to renew inter-pseudonym identity $IPID$ are saved in the TPD. Figure 4 explains the process of the pseudonym renew phase in detail.

- The vehicle V_i randomly picks a value α, computes $\xi_1 = \mathcal{T}_\alpha(x) mod$ P and computes public pseudonym identity $F_{v_i} = IPID_{v_i} \oplus h(A_{v_i}||T_{v_i}^2)$, where $T_{v_i}^2$ is the latest timestamp.
- The vehicle computes $B_{v_i}^1 = h(A_{v_i}||\xi_1||F_{v_i}||T_{v_i}^2)$ and sends the tuple $\{\xi_1, F_{v_i}, T_{v_i}^2, B_{v_i}^1\}$ to the TA through the 5G-BS.
- The TA first verifies the timestamp $T_{v_i}^2$ of the tuple $\{\xi_1, F_{v_i}, T_{v_i}^2, B_{v_i}^1\}$ and then checks the vehicle by checking whether the equation $B_{TA}^{-} = h(A_{v_i}||\xi_1||F_{v_i}||T_{v_i}^2) \stackrel{?}{=} B_{v_i}^1$ are equal.
- The TA seeks whether the member list has the inter-pseudonym identity $IPID_{v_i} = F_{v_i} \oplus h(A_{v_i}||T_{v_i}^2)$. If it is false, the process will be ended. Otherwise, the TA continues by checking the validity of SVP_{v_i}.

- The TA randomly picks a value β, computes $\xi_2 = \mathcal{T}_\beta(x) mod$ P and computes a new inter-pseudonym identity $IPID_{v_i}^{new} = h(OID_{v_i}||A_{v_i}||SVP_{v_i}^{new})$, where $SVP_{v_i}^{new}$ is a new short time period.
- The TA encrypts $IPID_{v_i}^{new}$ by using $\digamma_{TA} = IPID_{v_i}^{new} \oplus h(A_{v_i}||T_{TA}^3)$, computes $B_{TA}^2 = h(A_{v_i}||\xi_1||\xi_2||\digamma_{TA}||T_{v_i}^3)$ and then sends tuple $\{\xi_2, \digamma_{TA}, T_{v_i}^3, B_{TA}^2\}$ to the vehicle through the 5G-BS.
- The vehicle first verifies the timestamp $T_{v_i}^3$ of the tuple $\{\xi_2, \digamma_{TA}, T_{v_i}^3, B_{v_i}^2\}$ and then checks the TA by checking whether the equations $B_{v_i}^- = h(A_{v_i}||\xi_1||\xi_2||\digamma_{TA}||T_{v_i}^3) \stackrel{?}{=} B_{TA}^2$ are equal.
- The vehicle sets $IPID_{v_i}^{new}$ as the new inter-pseudonym identity by using $IPID_{v_i}^{new} = \digamma_{TA} \oplus h(A_{v_i}||T_{TA}^3)$.

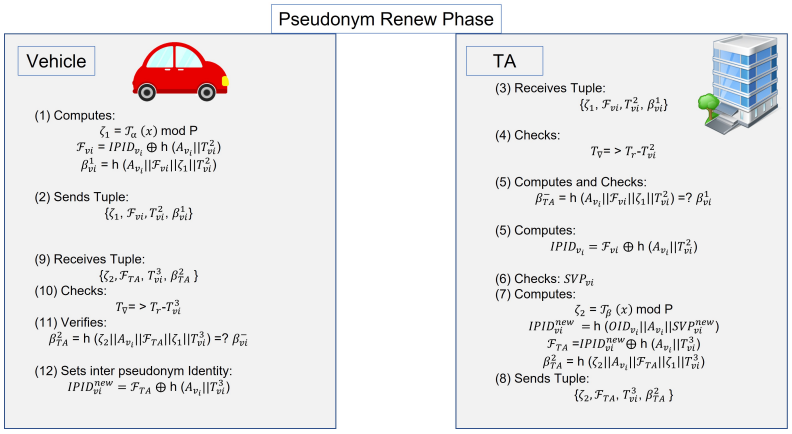


Figure 4. Pseudonym Renew Phase.

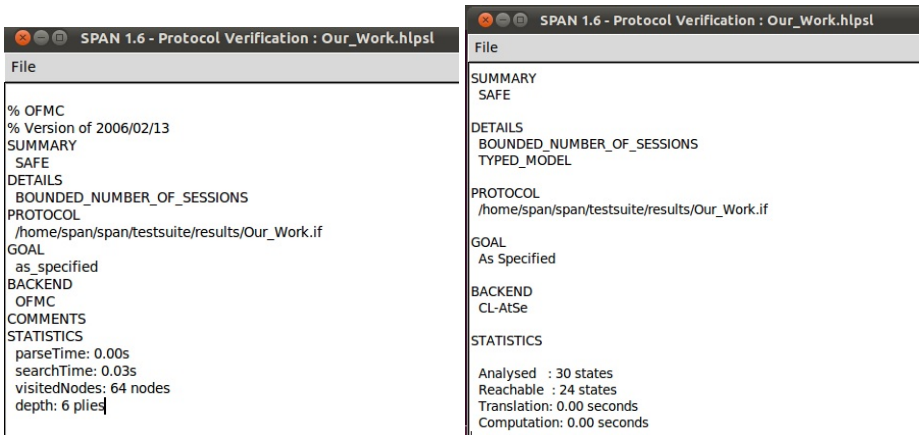
5. Security Analysis

In the following subsections, formal analysis, security proof, informal analysis, and security comparison of our work are presented.

5.1. Formal Analysis

AVISPA [33] is a software tool to automatically validate internet security applications and protocols. AVISPA is widely applied to provide a formal security analysis of the scheme. It has four back-ends that have a heterogeneity of mechanisms: (a) "Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP)", (b) "Constraint-logic-based Attack Searcher (CLAtSe)", (c) "SAT-based Model Checker (SATMC)" and (d) "On-the-fly mode-checker (OFMC)". A security scheme needs to be programmed utilizing the "High-Level Protocol Specification Language (HLPSL)" of AVISPA.

This paper runs the "Security Protocol ANimator for AVISPA (SPAN)" tool [34] for formal security analysis of our work. Figure 5 displays the simulation results of our work. Since both the TA4SP back-end and SATMC back-end do not currently support "bitwise XOR operations", the simulation of our work is based on the OFMC back-end and CL-AtSe back-end only. Note that the "Dolev-Yao threat model (DY model)" [35] is executed by SPAN/AVISPA. Thus, the third party has full power control through communication.



(**a**) (**b**)

Figure 5. The simulation results under OFMC and CL-AtSe back-ends. (**a**) OFMC back-end; (**b**) CL-AtSe back-end.

5.2. Security Proof

Theorem 1. *Suppose that the CPDHP problem according to the hash function is safe and extended mapping of chaotic is legal. Thus, under Definition 2, our work is the security key negotiation method.*

Proof. Let A be an attacker, utilize q_s to indicate the value of times the value queried the **Send**, utilize q_r to indicate the value of times the value queried the **Reveal**, and q_e to indicate the value of times the attacker queried the **Execute**. Construct a Challenger C to imitate the true protocol work via **Send** Oracle query. Describe Game $Game_i$: i = 0, 1, 2...; by continuously altering the Oracle replies of adjacent games, it can be shown that the diversity in the probability of an attacker gaining the game is negligible. □

In the last game, the probability of evaluating the adversary successfully was only $\frac{1}{2}$. Therefore, it is evaluated that the probability of win of the attacker method can be ignored. Assume that the event of Repeat represents that the scenario working example has chosen the x_i that has been chosen. The active event probability is:

$$Pr[Repeat] \leq \frac{(q_s)^2}{2^{k+1}} \tag{4}$$

Guess: Once all queries are completed, attacker A guesses b^- of b. Once b^- = b, then the attacker has broken the security of the system successfully. This event is indicated by $Succ_A$, and Att_A is described to indicate the attack advantage of any attacker A against the scheme, where $Att_A \overset{\text{def}}{=} [2Pr[Succ_A] - 1]$.

Game0: The challenger C replies to the attacker's query based on the execution operation of the true method. Thus, the probability of winning against the adversary is equal to the probability of win of the adversary attacking the true method. Hence, the following can be concluded:

$$Pr[E_0] = Pr[Succ_A] \tag{5}$$

Game1: In **Game1**, the Oracle will follow **Game0**. Once Repeat or Forge events occur, the challenger C ends the game. Hence, the following can be concluded:

$$Pr[E_1] - Pr[E_0]| \leq Pr[Forge] + Pr[Repeat] \tag{6}$$

Game2: In this game, for the Send($\sum_v^i, M_2$) query, the challenger C initially tests when the working example is Corrupt and successfully passes it to $\sum_v^i$, and the challenger C

randomly selects the signature to a random number SM_{vi}. Since the signature is a uniformly distributed random number; hence, the following can be concluded:

$$Pr[E_2] = \frac{1}{2} \tag{7}$$

By merging Equations (4)–(7), the following can be concluded:

$$\begin{aligned} Att_A &= |2 \cdot Pr[Succ_A] - 1| \\ &\leq \frac{(q_s)^2}{2^{k+1}} + 2Att_{dlp} + 2 \cdot q_s Att_{CPDHP} \end{aligned} \tag{8}$$

Ultimately, it is evaluated and proved that the attacker's probability of breaking the security of our work is negligible.

5.3. Informal Analysis

In this subsection, security goals should be satisfied in our work for 5G-enabled vehicular networks as below:

- Satisfying Pseudonym Identity: The vehicle's original identity OID_{v_i} is hidden with an inter-pseudonym identity $IPID_{vi}$ by the TA at the enrollment phase of our work. Before broadcasting the message to vehicle-to-everything (V2X) communication, the vehicle computes a public pseudonym identity $PPID_{v_i} = IPID_{v_i} \oplus h(A_{v_i}||T_{v_i})$, where T_{v_i} is the latest timestamp and then sends the message-tuple $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$. Therefore, our work is safe, and the adversary does not have the capability to attack the scheme to obtain the vehicle's identity from the message.
- Satisfying Authentication and Integrity: In our work, the recipient verifies the node authentication and message integrity by checking through $\mathcal{T}_{PPID_{v_i}.SM_{vi}^{-}}(Pr_{vi}) \stackrel{?}{=} \mathcal{T}_{PPID_{v_i}}(\sigma_{vi})$. After completing the verification process, the vehicle then accepts the safety-related message M_i included of the message-tuple $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$. Therefore, our work is achieving requirements of authentication and integrity in 5G-enabled vehicular networks.
- Satisfying Traceablility: The original identity of vehicle OID_{v_i} is hid in an inter-pseudonym identity $IPID_{vi}$, where $IPID_{v_i} = h(OID_{v_i}||A_{v_i}||SVP_{v_i})$. Due to the $IPID_{vi}$ being hid in $PPID_{vi}$ of the message-tuple $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$, the attacker does not have the ability to disclose it. The TA is only able to retrieve the original identity by computing $IPID_{v_i} = PPID_{v_i} \oplus h(A_{v_i}||T_{v_i})$, where A_{v_i} is stored on the TA. Therefore, our work is satisfying traceability requirement.
- Satisfying Unlinkability: In our work, the vehicle generates public pseudonym identity $PPID_{v_i} = IPID_{v_i} \oplus h(A_{v_i}||T_{v_i})$ by the chaotic map based a hash function h, and the adversary does not have the ability to determine two $PPID_{v_i}$ that are issued from the same enrolled vehicle. Hence, our work satisfies the unlinkability requirement in 5G-enabled vehicular networks.
- Resisting Side-Channel Attack: The assumption of the existing authentication scheme is that a TPD is not compromised by an adversary; thereby, the secret key of the system (TA) is preloaded and saved in the enrolled vehicle. Nevertheless, the adversary could conduct malicious activities by launching an attack on a side channel to acquire the sensitive data preserved on TPD. Then, the adversary impersonates a legal vehicle and sends fake messages to collapse the system of vehicular networks. In our work, before the short valid period SVP_{v_i} is to expire, the inter-pseudonym identity $IPID_{v_i}$ is regularly renewed to be new $IPID_{v_i}^{new}$ to resist side-channel attack. Therefore, our work is safe from the side-channel attack, and the adversary does not have the ability to attack the scheme to acquire the sensitive information saved on the TPD of enrolled vehicles in 5G-enabled vehicular networks.
- Resisting Replay Attack: The message-tuple $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ sent by the enrolled vehicle includes a timestamp T_{vi}; the recipient has the ability to check if the message is replayed by verifying the timestamp T_{vi}. Therefore, our work is safe for a replay

attack, and the adversary does not have the ability to attack the scheme to replay the message in 5G-enabled vehicular networks.

- Resisting Modify Attack: The message-tuple $\{PPID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ sent by the enrolled vehicle includes a signature σ_{vi}; the recipient has the ability to check if the message is modify by verifying the σ_{vi}, as shown in Equation (3). Therefore, our work is safe for modification attacks, and the adversary does not have the ability to attack the scheme to modify the message.
- Resisting Forgery Attack: During the enrollment phase of our work, after submitting the original identity of vehicle OID_{v_i}, the TA computes the inter-pseudonym identity $IPID_{v_i}$. Then, $IPID_{v_i}$ and A_{v_i} are preloaded to the enrolled vehicle by the TA. Therefore, no third party has the ability to retrieve the data saved to impregnate a legal vehicle. Therefore, our work is safe for forgery attacks, and the adversary does not have the ability to attack the scheme to impersonate the legal vehicle in 5G-enabled vehicular networks.
- Resisting Man-In-The-Middle attack: According to Section 5.1, the model of the Dolev–Yao threat is implemented by AVISPA. Therefore, our work is safe for a Man-In-The-Middle attack, and the adversary does not have the ability to attack the scheme to change/modify the message sent in 5G-enabled vehicular networks.

5.4. Security Comparison

In this section, a security comparison is made between the existing related schemes and our work. The outcome of the comparison is tabulated in Table 2, where src1, src2, src3, src4, src5, src6, src7, src8, and src9 indicate pseudonym identity, authentication, and integrity, traceability, unlinkability, replay attack, modify attack, forgery attack, Man-In-The-Middle (MITM) attack, and side-channel attack, respectively.

As is concluded in Table 2, the privacy and security requirements could be achieved in our work; nevertheless, side-channel attack could not be achieved in the schemes of Bayat et al. [25], Jianhong et al. [26], He et al. [28] and Wu et al. [29].

Table 2. Security comparison.

Schemes	src1	src2	src3	src4	src5	src6	src7	src8	src9
Bayat et al. [25]	✓	✓	✓	✓	✓	✓	✓	✓	✗
Jianhong et al. [26]	✓	✓	✓	✓	✓	✓	✓	✓	✗
He et al. [28]	✓	✓	✓	✓	✓	✓	✓	✓	✗
Wu et al. [29]	✓	✓	✓	✓	✓	✓	✓	✓	✗
Our work	✓	✓	✓	✓	✓	✓	✓	✓	✓

6. Efficiency Performance

In this section, efficiency performance is provided and compared between the related schemes and our work for vehicular networks. For convenience, the runtime of some different operations of cryptographic is described in Table 3. The specific configuration of the machine running the code of our work is in [36] to run on the 3.2 GH platform utilizing the Java Cryptography library to obtain the runtime of different cryptographic operations. The efficiency performance with regard to computation cost and communication costs is analyzed in the following two subsections.

Table 3. Runtime of different cryptographic operations.

Operations	Description	Time (ms)
$T_{pair-bp}$	The runtime of the BPC operation $\bar{e}$ (S, T).	1.537
T_{ptm}	The runtime of a Point-to-Map hashing operation for the BPC.	0.937
$T_{mul-ecc}$	The runtime of a scale multiplication operation $x.P$ for the ECC.	0.715
T_{chev}	The runtime of the Chebyshev's polynomial mapping operation.	0.341

6.1. Cost of Computation

The cryptographic operations in the schemes of Bayat et al. [25] and Jianhong et al. [26] are built on a bilinear pair, while the schemes of He et al. [28], Wu et al. [29] and Cui et al. [31] use ECC. In contrast, our work uses the Chebyshev polynomial-based scheme for resisting side-channel attacks in 5G-enabled vehicular networks. Table 4 presents the comparison of the signing and verifying messages and analyzed schemes comparison in Figure 6.

Table 4. Comparison of the signing and verifying messages.

Schemes	Signing Messages	Verifying Messages
Bayat et al. [25]	$T_{ptm} \approx 0.937$ ms	$3T_{pair-bp} + T_{ptm} \approx 5.548$ ms
Jianhong et al. [26]	$T_{ptm} \approx 0.937$ ms	$3T_{pair-bp} \approx 4.611$ ms
He et al. [28]	$3T_{mul-ecc} \approx 2.145$ ms	$3T_{mul-ecc} \approx 2.145$ ms
Wu et al. [29]	$2T_{mul-ecc} \approx 1.43$ ms	$4T_{mul-ecc} \approx 2.86$ ms
Cui et al. [31]	$3T_{mul-ecc} \approx 2.145$ ms	$3T_{mul-ecc} \approx 2.145$ ms
Our work	$2T_{chev} \approx 0.682$ ms	$3T_{chev} \approx 1.023$ ms

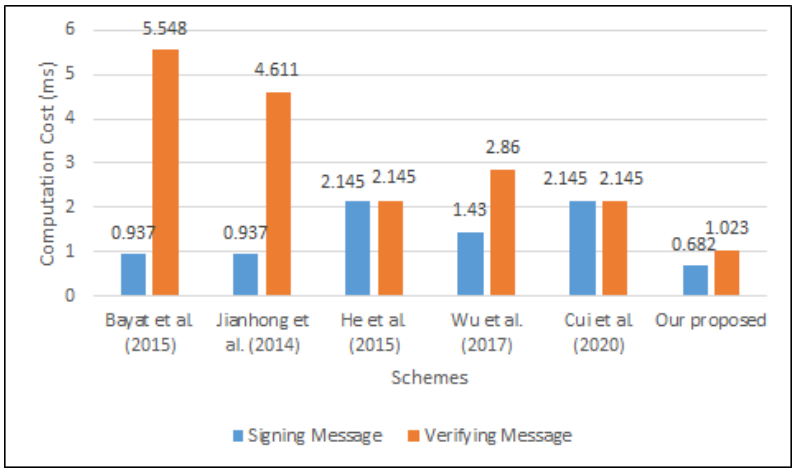


Figure 6. Analysed schemes comparison.

Before sending the message in the scheme of Bayat et al. [25], the enrolled vehicle requires one Point-to-Map hashing operation to perform the signing message process. Thereby, the entire runtime is $T_{ptm} \approx 0.937$ ms. Meanwhile, before accepting the message, the enrolled vehicle requires three BPC operations and one Point-to-Map hashing operation to perform the verifying message process. Thereby, the entire runtime is $3T_{pair-bp} + T_{ptm} \approx 5.548$ ms.

Before sending the message in the scheme of Jianhong et al. [26], the enrolled vehicle requires one Point-to-Map hashing operation to perform the signing message process. Thereby, the entire runtime is $T_{ptm} \approx 0.937$ ms. Meanwhile, before accepting the message, the enrolled vehicle requires three BPC operations to perform the verifying message process. Thereby, the entire runtime is $3T_{pair-bp} \approx 4.611$ ms.

Before sending the message in the scheme of He et al. [28], the enrolled vehicle requires three ECC operations to perform the signing message process. Thereby, the entire runtime is $3T_{mul-ecc} \approx 2.145$ ms. Meanwhile, before accepting the message, the enrolled vehicle requires three ECC operations to perform the verifying message process. Thereby, the entire runtime is $3T_{mul-ecc} \approx 2.145$ ms.

Before sending the message in the scheme of Wu et al. [29], the enrolled vehicle requires two ECC operations to perform the signing message process. Thereby, the entire runtime is $2T_{mul-ecc} \approx 1.43$ ms. Meanwhile, before accepting the message, the enrolled vehicle requires four ECC operations to perform the verifying message process. Thereby, the entire runtime is $4T_{mul-ecc} \approx 2.86$ ms.

Before sending the message in the scheme of Cui et al. [31], the enrolled vehicle requires three ECC operations to perform the signing message process. Thereby, the entire

runtime is $3T_{mul-ecc} \approx 2.145$ ms. Meanwhile, before accepting the message, the enrolled vehicle requires four ECC operations to perform the verifying message process. Thereby, the entire runtime is $3T_{mul-ecc} \approx 2.145$ ms.

Before sending the message in our work, the enrolled vehicle requires two Chebyshev polynomial operations to perform the signing message process. Thereby, the entire runtime is $2T_{chev} \approx 0.682$ ms. Meanwhile, before accepting the message, the enrolled vehicle requires three Chebyshev polynomial operations to perform the verifying message process. Thereby, the entire runtime is $3T_{chev} \approx 1.023$ ms.

As listed in Table 4, the cost of computation of our work is 0.682 ms, which decreases by $\frac{0.937-0.682}{0.937} \approx 27.21\%$, $\frac{0.937-0.682}{0.937} \approx 27.21\%$, $\frac{2.145-0.682}{2.145} \approx 68.21\%$, $\frac{1.43-0.682}{1.43} \approx 52.31\%$, and $\frac{2.145-0.682}{2.145} \approx 68.21\%$, respectively, against the schemes of Bayat et al. [25], Jianhong et al. [26], He et al. [28], Wu et al. [29] and Cui et al. [31] for the signing messages process. Meanwhile, during the verifying message process, the cost of computation of our work is 1.023 ms, which decreases by $\frac{5.548-1.023}{5.548} \approx 81.65\%$, $\frac{4.611-1.023}{4.611} \approx 77.81\%$, $\frac{2.145-1.023}{2.145} \approx 52.32\%$, $\frac{2.86-1.023}{2.86} \approx 64.23\%$, and $\frac{2.145-1.023}{5.548} \approx 52.32\%$, respectively, against the schemes of Bayat et al. [25], Jianhong et al. [26], He et al. [28], Wu et al. [29] and Cui et al. [31]. The performance of our work against other compared works to sign and verify messages is tabulated in Table 5.

Table 5. Cost of computation comparison.

Schemes	Signing Messages	Verifying Messages
Bayat et al. [25]	27.21%	81.65%
Jianhong et al. [26]	27.21%	77.81%
He et al. [28]	68.21%	52.32%
Wu et al. [29]	52.31%	64.23
Cui et al. [31]	68.21%	52.32%

6.2. Cost of Communication

This subsection analyzes authentication schemes by comparing the communication cost of the schemes of Bayat et al. [25], Jianhong et al. [26], He et al. [28], Wu et al. [29] and our work for vehicular networks. Generally, in a public channel environment for vehicular networks, the communication cost creates a message-tuple sent from a vehicle to others. Thereby, this paper supposes that the output of a hash function is 160 bits, the output of the timestamp is 32 bits, the output of the BPC point $P = (P_x, P_y)$ is (512 + 512) = 1024 bits, and the output of the ECC point is (160 + 160) = 320 bits. The size of the message is excluded in this process. The comparison of cost of communication is tabulated in Table 6 and the analyzed schemes are compared in Figure 7.

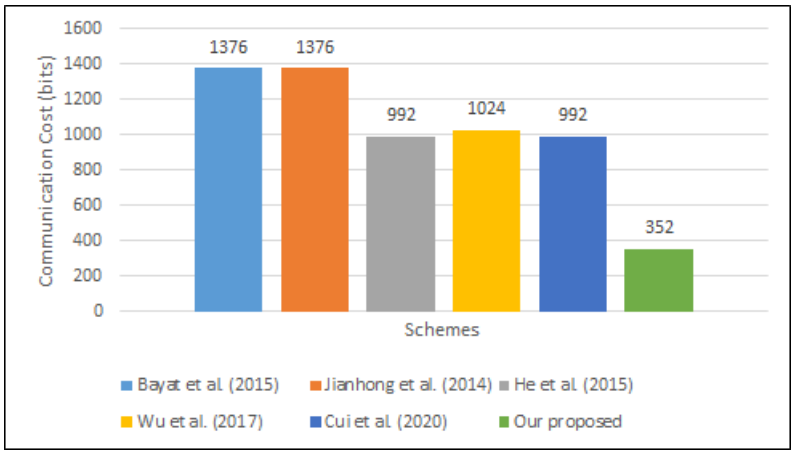


Figure 7. Cost of communication comparison.

As tabulated in Table 6, the cost of communication of our work is 352 bits, which decreases by $\frac{1376-352}{1376} \approx 74.42\%$, $\frac{1376-352}{1376} \approx 74.42\%$, $\frac{992-352}{992} \approx 64.52\%$, $\frac{1024-352}{1024} \approx 65.63\%$, and $\frac{992-352}{992} \approx 64.52\%$, respectively, against the schemes of Bayat et al. [25], Jianhong et al. [26], He et al. [28], Wu et al. [29] and Cui et al. [31].

Table 6. Comparison of cost of communication.

Schemes	Message Tuple	Size of Tuple (Bits)	Improvement
Bayat et al. [25]	$\{ID_1^i, ID_2^i, \sigma_i, T_i\}$	1024 + 160 + 160 + 32 = 1376	74.42%
Jianhong et al. [26]	$\{ID_1^i, ID_2^i, \sigma_i, T_i\}$	1024 + 160 + 160 + 32 = 1376	74.42%
He et al. [28]	$\{AID_{i,1}, AID_{i,2}, T_i, R_i, \sigma_i\}$	320 + 160 + 32 + 320 + 160 = 992	64.52%
Wu et al. [29]	$\{PID_{vi}, T_i, T_{vi}, h_{ki}, R_i, \sigma_i\}$	320 + 32 + 32 + 160 + 320 +160 = 1024	65.63%
Cui et al. [31]	$\{PID_j, DT_{ij}, \sigma_j, D_j, T_j\}$	320+320+160+160 +32 = 992	64.52%
Our work	$\{PPID_{vi}, T_{vi}, \sigma_{vi}\}$	160 + 32 + 160 = 352	

7. Conclusions

In this paper, the Chebyshev polynomial-based scheme for resisting side-channel attacks in 5G-enabled vehicular networks could achieve both important properties in terms of chaotic and semi-group. Compared with other methods, our work can thwart the side-channel attack by periodically renewing the sensitive data preserved on the TPD on the enrolled node's OBU. Our work is also proven to be secure against the model of Dolev–Yao attacks in the AVISPA simulator. Security analysis shows that our work archives all of the design goals with regard to privacy (pseudonym identity and unlikability) and security (authentication, integrity, and traceability) in 5G-enabled vehicular networks. Nevertheless, the resistance to side-channel attacks could not be achieved in the relevant works. Ultimately, since our work does not employ BPC and ECC operations, the efficiency performance of our work is the lowest compared to the four related schemes. Thus, our work has better efficiency with regard to costs of computation and communication.

In future work, we will carry out the simulation experiment of the proposed scheme by running a traffic simulator (SUMO) and a network simulator (OMNeT++) to provide more performance details in terms of varying the speed and numbers of UE. Moreover, we plan to explore achieving the privacy and security factors in a more dynamic scenario containing fog computing technology over 5G communication.

Author Contributions: Conceptualization, writing—review and editing, M.A.A.-S.; writing—original draft preparation, investigation, supervision, S.M.; funding acquisition, software, visualization, B.A.M.; methodology, funding acquisition, resources, Z.G.A.-M.; project administration, funding acquisition, software, A.Q.; funding acquisition, investigation, resources, A.J.A.; data curation, software, visualization, G.A.; visualization, methodology, visualization, supervision, A.A.S.; and investigation, methodology, validation, K.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been funded by the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, through project number RG-21098.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to acknowledge the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, for funding this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chiti, F.; Fantacci, R.; Giuli, D.; Paganelli, F.; Rigazzi, G. Communications protocol design for 5G vehicular networks. In *5G Mobile Communications*; Springer: Cham, Switzerland, 2017; pp. 625–649.
2. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. SE-CPPA: A Secure and Efficient Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. *Sensors* **2021**, *21*, 8206. [CrossRef] [PubMed]
3. Wymeersch, H.; Seco-Granados, G.; Destino, G.; Dardari, D.; Tufvesson, F. 5G mmWave positioning for vehicular networks. *IEEE Wirel. Commun.* **2017**, *24*, 80–86. [CrossRef]
4. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Khalil, A.; Hasbullah, I.H. Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey. *IEEE Access* **2021**, *9*, 121522–121531. [CrossRef]
5. Ge, X.; Li, Z.; Li, S. 5G software defined vehicular networks. *IEEE Commun. Mag.* **2017**, *55*, 87–93. [CrossRef]
6. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. A Secure Pseudonym-Based Conditional Privacy-Preservation Authentication Scheme in Vehicular Ad Hoc Networks. *Sensors* **2022**, *22*, 1696. [CrossRef]
7. Alazzawi, M.A.; Al-behadili, H.A.; Srayyih Almalki, M.N.; Challoob, A.L.; Al-shareeda, M.A. Id-ppa: Robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network. In Proceedings of the International Conference on Advances in Cyber Security, Penang, Malaysia, 8–9 December 2020; pp. 80–94.
8. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Password-Guessing Attack-Aware Authentication Scheme Based on Chinese Remainder Theorem for 5G-Enabled Vehicular Networks. *Appl. Sci.* **2022**, *12*, 1383. [CrossRef]
9. Cincilla, P.; Hicham, O.; Charles, B. Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios. In Proceedings of the IEEE Vehicular Networking Conference (VNC), Columbus, OH, USA, 8–10 December 2016; pp. 1–8.
10. Huang, D.; Misra, S.; Verma, M.; Xue, G. PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 736–746. [CrossRef]
11. Joshi, A.; Gaonkar, P.; Bapat, J. A reliable and secure approach for efficient car-to-car communication in intelligent transportation systems. In Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2017; pp. 1617–1620.
12. Lu, R.; Lin, X.; Luan, T.H.; Liang, X.; Shen, X. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Trans. Veh. Technol.* **2011**, *61*, 86–96. [CrossRef]
13. Thenmozhi, T.; Somasundaram, R. Pseudonyms based blind signature approach for an improved secured communication at social spots in VANETs. *Wirel. Pers. Commun.* **2015**, *82*, 643–658. [CrossRef]
14. Rajput, U.; Abbas, F.; Oh, H. A hierarchical privacy preserving pseudonymous authentication protocol for VANET. *IEEE Access* **2016**, *4*, 7770–7784. [CrossRef]
15. Asghar, M.; Doss, R.R.M.; Pan, L. A scalable and efficient PKI based authentication protocol for VANETs. In Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, 21–23 November 2018; pp. 1–3.
16. F´orster, D.; Kargl, F.; L`ohr, H. PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET). In Proceedings of the IEEE Vehicular Networking Conference (VNC), Paderborn, Germany, 3–5 December 2014; pp. 25–32.
17. Sun, Y.; Zhang, B.; Zhao, B.; Su, X.; Su, J. Mix-zones optimal deployment for protecting location privacy in VANET. *Peer -Peer Netw. Appl.* **2015**, *8*, 1108–1121. [CrossRef]
18. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A Threshold Anonymous Authentication Protocol for VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1711–1720. [CrossRef]
19. Alimohammadi, M.; Pouyan, A.A. Sybil attack detection using a low cost short group signature in VANET. In Proceedings of the 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Rasht, Iran, 8–10 September 2015; pp. 23–28.
20. Zhang, L.; Wu, Q.; Qin, B.; Domingo-Ferrer, J.; Liu, B. Practical secure and privacy-preserving scheme for value-added applications in VANETs. *Comput. Commun.* **2015**, *71*, 50–60. [CrossRef]
21. Cui, J.; Wang, Y.; Zhang, J.; Xu, Y.; Zhong, H. Full Session Key Agreement Scheme Based on Chaotic Map in Vehicular Ad hoc Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8914–8924. [CrossRef]
22. Lim, K.; Tuladhar, K.M.; Wang, X.; Liu, W. A scalable and secure key distribution scheme for group signature based authentication in VANET. In Proceedings of the IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 19–21 October 2017; pp. 478–483.
23. Zhang, C.; Lu, R.; Lin, X.; Ho, P.H.; Shen, X. An efficient identity-based batch verification scheme for vehicular sensor networks. In Proceedings of the IEEE INFOCOM 2008-The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 246–250.
24. Lee, C.C.; Lai, Y.M. Toward a secure batch verification with group testing for VANET. *Wirel. Netw.* **2013**, *19*, 1441–1449. [CrossRef]
25. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A secure authentication scheme for VANETs with batch verification. *Wirel. Netw.* **2015**, *21*, 1733–1743. [CrossRef]
26. Jianhong, Z.; Min, X.; Liying, L. On the security of a secure batch verification with group testing for VANET. *Int. J. Netw. Secur.* **2014**, *16*, 351–358.

27. Zhang, L.; Wu, Q.; Domingo-Ferrer, J.; Qin, B.; Hu, C. Distributed aggregate privacy-preserving authentication in VANETs. *IEEE Trans. Intell. Transp. Syst.* **2016**, *18*, 516–526. [CrossRef]
28. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
29. Wu, L.; Fan, J.; Xie, Y.; Wang, J.; Liu, Q. Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717700899. [CrossRef]
30. Cui, J.; Xu, W.; Han, Y.; Zhang, J.; Zhong, H. Secure mutual authentication with privacy preservation in vehicular ad hoc networks. *Veh. Commun.* **2020**, *21*, 100200. [CrossRef]
31. Cui, J.; Chen, J.; Zhong, H.; Zhang, J.; Liu, L. Reliable and Efficient Content Sharing for 5G-Enabled Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 1247–1259. [CrossRef]
32. Cui, J.; Zhang, X.; Zhong, H.; Ying, Z.; Liu, L. RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks. *IEEE Internet Things J.* **2019**, *6*, 6417–6428. [CrossRef]
33. Armando, A.; Basin, D.; Boichut, Y.; Chevalier, Y.; Compagna, L.; Cuéllar, J.; Drielsma, P.H.; Héam, P.C.; Kouchnarenko, O.; Mantovani, J.; et al. The AVISPA tool for the automated validation of internet security protocols and applications. In Proceedings of the International Conference on Computer Aided Verification, Edinburgh, UK, 6–10 July 2005; pp. 281–285.
34. Glouche, Y.; Genet, T.; Heen, O.; Courtay, O. A security protocol animator tool for AVISPA. In Proceedings of the ARTIST2 Workshop on Security Specification and Verification of Embedded Systems, Pisa, Italy, 18–20 May 2006.
35. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
36. Roychoudhury, P.; Roychoudhury, B.; Saikia, D.K. Provably secure group authentication and key agreement for machine type communication using Chebyshev's polynomial. *Comput. Commun.* **2018**, *127*, 146–157. [CrossRef]