CM-CPPA: Chaotic Map-Based Conditional Privacy-Preserving Authentication Scheme 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, Gelugor 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.: +60-4-653-3004

Abstract: The security and privacy concerns in vehicular communication are often faced with schemes depending on either elliptic curve (EC) or bilinear pair (BP) cryptographies. However, the operations used by BP and EC are time-consuming and more complicated. None of the previous studies efficiently tackled the efficient performance of signing messages and verifying signatures. Therefore, a chaotic map-based conditional privacy-preserving authentication (CM-CPPA) scheme is proposed to provide communication security in 5G-enabled vehicular networks in this paper. The proposed CM-CPPA scheme employs a Chebyshev polynomial mapping operation and a hash function based on a chaotic map to sign and verify messages. Furthermore, by using the AVISPA simulator for security analysis, the results of the proposed CM-CPPA scheme are good and safe against general attacks. Since EC and BP operations do not employ the proposed CM-CPPA scheme, their performance evaluation in terms of overhead such as computation and communication outperforms other most recent related schemes. Ultimately, the proposed CM-CPPA scheme decreases the overhead of computation of verifying the signatures and signing the messages by 24.2% and 62.52%, respectively. Whilst, the proposed CM-CPPA scheme decreases the overhead of communication of the format tuple by 57.69%.

Keywords: 5G-enabled; Chebyshev polynomial; chaotic map; vehicular networks; privacy and security

1. Introduction

The vehicular ad hoc networks (VANETs) aim to provide drivers and passengers with smarter, safer, and more entertainment services. In the coming fifth-generation (5G) era, the participating vehicle in the vehicular network is investigated to be installed with an on-board unit (OBU) for vehicle-to-everything (V2X) communication [1–3]. Therefore, the vehicle can exchange messages with others and the outside world.

Currently, the number of urban automobiles is quickly increasing, and the demands of drivers are diversifying. Thus, the VANET under the 5G mobile networks can satisfy the characteristics of high bandwidth and wide coverage for the current application environment. It presents a plethora of challenges as well as opportunities for vehicular networks [4–6]. Under 5G wireless networks, the characteristics are 20 Gb/s and 100 Mb/s for data transmission and average data transmission rates, respectively [7,8].

Nevertheless, owing to the nature of wireless communication as a public channel, the exchanged messages among vehicles might be modified when adversaries exist. Privacy and security vulnerabilities are critical requirements in a 5G-enabled vehicular...
Regardless of privacy and security requirements, effective performance is also critical in V2X communication. For example, when there are 100 nodes within the Covered zone of the vehicle, the receiver demands to verify 334–1500 messages per second. All the data shared by a vehicle can obviously be signed and verified by using cryptography operations to secure communication. However, the most recent conditional privacy-preserving authentication (CPPA) schemes are using operations elliptic curve (EC) or bilinear pair (BP) cryptographies to verify the signatures and sign messages. So, these operations are considered to be more complicated and time-consuming, and these cryptography algorithms are not suitable to be deployed in a 5G-enabled vehicular network.

The motivation behind this paper is to cope with this issue of effective performance during the signing and verifying messages caused by complicated and time-consuming operations. Therefore, this paper will propose a chaotic map-based CPPA scheme for vehicular networks relying on 5G technology. The proposed CM-CPPA scheme employs Chebyshev polynomial mapping operations to secure V2x communication.

To the best of the authors’ knowledge, Chebyshev polynomial mapping operations have not been used for CPPA schemes to date in the literature in 5G-enabled vehicular networks. More precisely, the following is a list of this paper’s key contributions:

- A chaotic map-based CPPA scheme is proposed for vehicular networks relying on 5G technology to achieve security goals in terms of piracy (Identity-Anonymity and Unlinkability) and security (Message Integrity and Authentication and Traceability) requirements. Moreover, our proposal has the ability to resist security attacks, such as modification, impersonation, replay, and man-in-the-middle.
- A scheme that applies chaotic polynomial map to generate/sign message (e.g., signer side) and verify the validity and authenticity of signature (e.g., checker side).
- A scheme that uses the well-known accepted simulator called AVISPA tool under OFMC and CL-AtSe back ends and shows that the scheme is perfectly secure against active and passive attacks.
- A scheme that outperforms most recent related schemes based on EC and BP operations with regard to overhead of computation and communication.

Here is how the remainder of the paper is organized. Section 2 discusses some CPPA schemes. Network structure, security goals and attackers model are explained in Section 3. Section 4 introduces the proposed CM-CPPA scheme. The security proof and performance metric of the proposed CM-CPPA scheme are given in Sections 5 and 6, respectively. Ultimately, Section 7 provides the conclusion of our proposal.

2. Related Work

In this section, some CPPA schemes for vehicular networks are discussed to secure wireless communication instead of public wireless communication.

Raya and Hubaux [12] proposed an approach that is based on anonymous certificates of users instead of the true identities for achieving the exchanged information integrity check. Digital signatures were used in this approach regarding to public key infrastructure (PKI) to introduce the CPPA schemes [12–21]. In vehicular networks, the PKI-based scheme is a sophisticated choice due to exchange of information that has not yet been determined as reliable and is purposed to be authenticated [10]. However, its limitations are also evident as follows: (i) a tremendous quantity of anonymous certificates are preloaded to each participating registered vehicle for achieving privacy; (ii) a great deal of private/public key pairs are stored in each vehicle, which needs a lot of storage capacities; (iii) all private/public key pairs and anonymous certificates for all participating vehicles are also required to store the trusted authority (TA), which causes burden storage for TA; (iv) disclosing the true identities of misbehaving vehicles in massive registration vehicle lists can also be exhausting.
With the purpose of settling the issues of the PKI-based approach, some researchers proposed an identity (ID) approach in vehicular networks. Instead of preloading a tremendous quantity of pairs (e.g., private/public key) and the relevant certificates, the identification is applied as the vehicle’s key of public, while private keys are issued by a TA utilizing the same identification and then preloaded to participating registered vehicles. The participating registered vehicle signs the message by employing its private key, whereas the verifier checks the integrity and authenticity of the message sent by utilizing the public key of the node. Zhang et al. [22] constructed authentication schemes by supporting the batch verification process to test the validity of multiple messages simultaneously in vehicular communication. Lee and Lai [23] identified two main limitations of the scheme proposed by Zhang et al. [22]. In the first limitation, the node can issue a forged identification to avoid the traceability property. In the second limitation, the impersonation attack is not resisted. To tackle the two limitations, Lee and Lai [23] designed an enhanced ID-based scheme to satisfy the top-level of security in vehicular communication. Jianhong et al. [24] also highlighted two main limitations of the scheme proposed by Lee and Lai [23], in which the non-repudiation property is not satisfied, and the replay attacks are not resisted. To tackle the two limitations, Jianhong et al. [24] provided an enhanced ID-based scheme to satisfy much higher effectiveness. Recently, some authentication schemes have been proposed by [25–30] to tackle privacy and security properties for vehicular networks. Furthermore, the ID-based schemes [25–31] use cryptography operations related to the Bilinear Pair (BP) to verify signatures and sign messages. Nevertheless, the operations of BP are complicated and time-consuming, which creates massive performance overheads with regard to overheads of communication and computation to verify signatures and sign messages. For instance, the participating registered vehicle in the Pournaghi et al. scheme [30] needs one bilinear pair operation and one Point-to-Map hashing for message signing, whereas the verifier needs three bilinear pair operations and one hashing (e.g., Point-to-Map) for message verification.

To overcome the time-consuming operations of ID-based BP approaches, He et al. [32] proposed an ID-based elliptic curve (EC) Cryptography to provide a signature verification process for vehicular communication. Recently, some authentication schemes based on EC have been proposed by [32–39] to tackle privacy and security properties for vehicular communication. Nevertheless, the operations of EC are time-consuming with an increase in the number of participating nodes. Therefore, Cui et al. [40] designed an ID-based scheme by adopting a Chaotic Map to sign and verify messages for the VANET. However, Cui et al. [40] used equipment called road-side unit (RSU) for authentication purposes, and RSU is more expensive and often needs thousands of dollars. To remove the used RSU, the most recent existing schemes use a 5G-enabled-vehicular network [41–43]. However, these schemes use time-consuming EC operations.

In the PKI approach, the vehicle saves large numbers of key pairs and the relevant certificate into OBU. Then, the vehicle selects randomly one of these parameters to verify the signature and sign the message. Unlike the PKI approach, the vehicle in our proposal only saves the master key of the system and public parameters. Thus, the vehicle uses the master key to generate the signature and compute a pseudonym for each communication in vehicular communication relying on 5G technology. To tackle the above issues arising in the vehicular communication, this paper proposes a chaotic map-based CPPA scheme for vehicular communication relying on 5G technology. Our proposal employs Chebyshev polynomial mapping operations instead of EC and BP operations for the signature verification process.

3. Background

This section presents the preliminaries for the proposed CM-CPPA scheme for vehicular communication relying on 5G technology with regards to the network structure, security goals, and attackers model as follows.
3.1. Network Structure

In this section, the explanation of the network structure of our proposal is given, which includes three network components: (1) TA; (2) 5G-BS; and (3) vehicle. The following steps are a brief explanation of these components, as presented in Figure 1.

Figure 1. Network Structure of vehicular communication relying on 5G technology [44].

- **TA**: Suppose that TA is full trust and has high resources with regard to computation capacity, sufficient storage, and high credibility. In the proposed CM-CPPA scheme, TA is in charge of generating security parameters (chaotic map) and preloading them to participating registered vehicles during the registration process. Furthermore, the TA saves its private key to the vehicle security. If the attacker compromises the TA, the entire system will be insecure. Additionally, the TA has the ability to update the parameters and then preload them into the vehicle to avoid any attack occurring.

- **5G-BS**: The 5G-BS is a wireless infrastructure mounted along the sides of roads. Suppose that 5G-BS is hard to be compromised. In the proposed CM-CPPA scheme, 5G-BS only acts as an intermediary transmission medium between the nodes and the TA without any storage or verification.

- **Vehicle**: Each vehicle has OBU for communicating with each other and sharing traffic information. A tamper-proof device (TPD) is fitted in each OBU to save critical data received from TA.

3.2. Security Goals

This subsection describes security goals that will be achieved by the proposed CM-CPPA scheme for vehicular communication relying on 5G technology.

- **Privacy (Identity-Anonymity)**: A true identification of the node must become fully anonymous to all participating registered vehicles.

- **Message Integrity and Authentication**: The recipient of a message has the ability to validate that the received message has not been changed by an adversary. Furthermore, the recipient of the message can check that it was issued by a participating registered vehicle.

- **Traceability**: In vehicular communication relying on 5G technology, the TA has the capability to track down the true identity of the sender in case of a dispute.

- **Unlinkability**: A third party should not be capable of relating several messages or predicting that these were issued by the same sender.
• Resistance to Security Attacks includes: modification, replay, impersonation, and man-in-the-middle attacks.

3.3. Attackers Model

Since the message is shared by the vehicle in a public channel, the attacker has the ability to fully control the message by changing, modifying, and replaying it to achieve their own malicious benefit. Security and privacy issues are both serious challenges in vehicular networks. To propose any sophisticated CPPA scheme, the following attacks must be resisted carefully.

• Modification Attack: The message shared by the vehicle can be modified/altered by the attacker to disturb the system.
• Impersonation Attack: The true identification of the node can be impersonated by an attacker to broadcast a forged message in the system.
• Replay Attack: The message shared by vehicles can be replied to at different times to send it again to other vehicles.
• Man-In-The-Middle Attack: The data shared between the recipient and sender can be interrupted by a third party to make damage to the entire system.

4. Proposed Scheme

This section presents the proposed CM-CPPA scheme without using the BP or EC operations. As displayed in Figure 2, the four main phases included in the proposed CM-CPPA scheme for vehicular communication relying on 5G technology: the system initialization, offline registration, message generation, and message verification phases. The notations applied in our proposal are defined by the subsequent expression.

![Figure 2. The Proposed CM-CPPA Scheme Phases.](image)

- Consider $P$ be a large prime number and $n$ be an integer.
- Consider $x$ be an inconstant tacking value in the interval $[-\infty, \infty] \rightarrow [-\infty, \infty]$.
- Consider $T_n(.)$ be a chaotic map (e.g., Chebyshev polynomial) of class $n$, which it is determined according to Equation (1).

$$\cos(n \cdot \arccos(x)) = T_n(x)$$ (1)
• The form of recurrence of the chaotic map $T_n : R \rightarrow R$ is as Equation (2).

$$2xT_{n-1}(x) - T_{n-2}(x)(modP), (n \geq 2) \equiv T_n(x)$$

where $T_1(x) = x$ and $T_0(x) = 1$. Additionally, a few instances of the chaotic map are given by Equation (3).

$$T_4(x) = 8x^4 - 8x^2 + 1,$$
$$T_3(x) = 4x^3 - 3x,$$
$$T_2(x) = 2x^2 - 1$$

• Chaotic feature: If degree $1 < n$, it can determine the chaotic map $T_w : [-\infty, \infty] \rightarrow [-\infty, \infty]$ with a fixed thickness $f^*(y) = 1/(\pi \sqrt{1 - y^2})$ function.

• Semi-group feature:

$$T_w(T_l(x)) = \cos(w\cos^{-1}(\cos(l\cos^{-1}(x)))) = \cos(wl\cos^{-1}(x)) = T_{wl}(x) = T_l(T_w(x))$$

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

• Discrete Logarithm (DL) problem: The major function of DL is to detect the unknown number $w$ such that $T_w(x) \equiv y$ for two taking items $y$ and $x$.

• Diffie–Hellman (DH) problem: The major function of DH is to evaluate the $T_{wl}(x)$ for three taking items $x, T_l(x)$, and $T_w(x)$.

• $h$: The chaotic map-based hash function, where $h : [-0, 1]^* \rightarrow [-0, 1]^l$.

• $TID_{vi}$: The identity of the vehicle.

• $||$: The operation of message concatenation.

• $\oplus$: The operation of exclusive-OR.

• $M_i$: The information-related message.

• $PID_{vi}$: The pseudonym-identification of the vehicle.

• $\sigma_{vi}$: The signature of the safety-related message $M_i$.

• $T_{vi}$: The current timestamp.

4.1. System Initialization Phase

In this phase, the TA is in charge of issuing system parameters (such as the chaotic map defined on it) before the deployment of 5G-enabled vehicular networks. This phase can be mathematically modeled by the subsequent steps.

• TA randomly picks values $x, k_s$ and the large prime $P$ based on the chaotic map in the whole system.

• TA randomly picks a value $s$ as its private key.

• TA chooses a chaotic map-based hash function $h$, where $h : [-0, 1]^* \rightarrow [-0, 1]^l$.

• TA sets $params = \{x, k_s, P, h\}$ as the public parameters.

4.2. Offline Registration Phase

In this phase, the vehicle $V_i$ executes the registration process at the system (TA) before leaving the factory. Based on the identity of vehicle $V_i$, the system parameters based on a chaotic map are preloaded to participating vehicles in 5G-enabled vehicular networks through a secure channel. The vehicle $V_i$ executes the offline registration phase by the subsequent steps.

• The driver submits the true identity of vehicle $TID_{vi}$ to the local TA.

• Once receiving $TID_{vi}$, the TA saves it to the list of vehicle registration.
• TA preloads the public parameters \( \text{params} = \{x, k_s, P, h\} \) to the vehicle \( V_i \).

• Finally, TA saves its private key \( s \) to the TPD of vehicle \( V_i \).

Note that sensitive data are stored in TPD, which will be never disclosed. Therefore, the adversary cannot successfully launch any attack to retrieve the private key of the system in the proposed CM-CPP A scheme. Additionally, our proposal only supports offline registration rather than online registration in order to avoid any insider attack in the system. Once this attack accrued, the forged message broadcasts to all vehicles to disrupt the system. Therefore, before the vehicle leaves the factory, the above steps should be carefully executed.

4.3. Message Generation Phase

In this phase, the TPD of vehicle \( V_i \) issues a pseudonym-ID \( PID_{vi} \) and signature \( \sigma_{vi} \) of safety-related message \( M_i \). After that, vehicle \( V_i \) broadcasts the pseudonym-ID \( PID_{vi} \), the message \( M_i \), and the signature \( \sigma_{vi} \) to neighboring nodes in 5G-enabled vehicular networks. As shown in Figure 3, the subsequent steps are executed by the vehicle \( V_i \) in this phase.

- \( V_i \) issues safety-related message \( M_i \) and the current timestamp \( T_{vi} \).
- \( V_i \) generates pseudonym-ID \( PID_{vi} = TID_{vi} \oplus h(s||T_{vi}) \).
- \( V_i \) computes the parameter \( SK_{vi} = T_{PID_{vi},s}(x) \mod P \).
- \( V_i \) signs the message \( SM_{vi} = h(M_i||PID_{vi}||T_{vi}) \).
- \( V_i \) computes the signature of safety-related message \( \sigma_{vi} = T_{SM_{vi}}(SK_{vi}) \mod P \).
- Finally, \( V_i \) broadcasts the message-tuple \( \{PID_{vi}, M_i, T_{vi}, \sigma_{vi}\} \) to the participating vehicles nearby in 5G-enabled vehicular networks.

![Figure 3. Message Generation and Verification Phases.](image)

4.4. Message Verification Phase

In this phase, the verifier \( V_j \) can authenticate and validate the signature of a safety-related message before accepting the message for further processing. By utilizing the message verification, no adversary has the ability to impersonate a participating registered vehicle and avoid false message transmission. As shown in Figure 3, the message verification is described by the subsequent steps.

- When receiving the message-tuple \( \{PID_{vi}, M_i, T_{vi}, \sigma_{vi}\} \), the verifier \( V_j \) initially checks the freshness of timestamp \( T_{vi} \).
- Then, the verifier \( V_j \) computes \( SM_{vj} = h(M_i||PID_{vi}||T_{vi}) \).
- Finally, the verifier \( V_j \) uses the message signature \( \sigma_{vi} \) of the message-tuple \( \{PID_{vi}, M_i, T_{vi}, \sigma_{vi}\} \) to check the safety-related message \( M_i \), where \( \sigma_{vi} = T_{SM_{vi}}(SK_{vi}) \mod P \).

The verifier \( V_j \) accepts the message if Equation (4) holds. Otherwise, the message is discarded.
\[ T_{PID_{v_j}}(v_{vi}) = T_{PID_{v_j},SM_{v_i}}(S_{K_{v_i}}) \]  

(4)

5. Security Analysis

In this section, the formal (AVISPA simulator) security proof and informal security analysis of the proposed CM-CPPA scheme are evaluated in detail in the following two subsections.

5.1. AVISPA

In this subsection, formal security verification of the proposed scheme is done utilizing the well-known “automated verification internet security protocol and applications (AVISPA)” simulator tool for ensuring that the proposed scheme is secure against all attacks. In AVISPA, each player performs a specific role since it is a role-based simulator. The specifications of simulation experiment parameters for AVISPA that had been used are explained as follows. The main tool SPAN Version 1.6 is based on Windows 7 Pro operating system (64 bit) that is running by SPAN-Ubuntu10.10-light on Oracle VirtualBox 6.1, Intel (R) Core (TM) 2.90 GHz processor i7-7500U CPU @ 2.70 GHz and 16 GB RAM.

To validate the proposed CM-CPPA scheme utilizing the AVISPA tool, initially, the proposed scheme is coded by using HLPSL. Then, the HLPSL2IF translator translates the HLPSL code to an IF, where IF is a lower-level language compared to HLPSL. Lastly, the IF specification is utilized directly by the back ends for analyzing whether the security goals are fulfilled or not. According to the output, the AVISPA simulator produces the result either in SAFE or UNSAFE mode against man-in-the-middle attacks and replay attacks. In the current version, the AVISPA simulator offers four types of the following back-ends verification tools: SATMC, CL-AtSe, OFMC, and TA4SP.

The authentication and broadcasting phases for the proposed CM-CPPA scheme are coded in HLPSL using two basic roles for an OBU and RSU. This process defines the session, environment, and goal as the compulsory roles. Figure 4 shows the simulation results of the proposed CM-CPPA scheme that resists the man-in-the-middle and replay attacks under the OFMC, and CL-AtSe back ends.

Figure 4. The simulation results under OFMC and CL-AtSe Back Ends. (a) OFMC back end; (b) CL-AtSe back end.

5.2. Security Proof

In this section, we provide the security proof of our proposal. The security model is defined as in [40].
Theorem 1. Consider that the DHP problem based on the hash function is secure and the expanded chaotic mapping is legitimated. Subsequently, according to the DHP problem, the FC-CPPA proposal is the security key negotiation process.

Proof. Let A represent an attacker, apply $q_k$ to show the amount queried by Send, apply $q_s$ to show the amount queried by Reveal, and $q_e$ represents the amount of times A queried by Execute. Build a Challenger $C$ to simulate the strong proposal run through a Send Oracle query. Depict Game $Game_i$: $i = 0, 1, 2 \ldots$, by everlastingly modifying the Oracle answers of adjacent games; it can be presented by the difference in the probability of $A$ obtaining the negligible game.

For the end game, the probability of analyzing $A$ profitably was only $\frac{1}{2}$. Thus, it is estimated that the probability of a win of the $A$ process can be neglected. Considering the event of Repeat indicates that the simulation running instance has picked the $x_i$ that has been picked. The probability of the strong event is:

$$Pr[Repeat] \leq \left(\frac{q_k}{2^{k+1}}\right)^2 \quad (5)$$

Guess: Once these queries are executed, $A$ outputs guess $b^*$ of $b$. Once $b^* = b$, then $A$ has broken the system security properly. This event is represented by $Succ_A$, and $Att_A$ has identified the attack feature of any $A$ against the scheme, where $Att_A[2Pr[Succ_A] - 1]$.

**Game1:** $C$ answers to $A$’s query according to the running cost operation of the strong process. So, the gaining probability against the $A$ attacking the real process. Thereby, we can conclude:

$$Pr[E_0] = Pr[Succ_A] \quad (6)$$

**Game2:** In game $Game_2$, all Oracle will rely on $Game_1$. Once Forge or Repeat events come, $C$ finishes the game. So, we can conclude:

$$Pr[E_1] - Pr[E_0] \leq Pr[Repeat] + Pr[Forge] \quad (7)$$

**Game3:** In game $Game_3$, for the $Send(\sum_i M_2)$ query, $C$ first verifies when the running instance is Corrupt and properly passes it to $\sum_i$, and $C$ picks randomly the signature to a random value $SM_{vi}$. Since the signature is a uniformly distributed random value, we can conclude:

$$Pr[E_2] = \frac{1}{2} \quad (8)$$

By combining Equations (4)–(7), we can conclude:

$$Att_A = |2 \cdot Pr[Succ_A]| \leq \left(\frac{q_k}{2^{k+1}}\right)^2 + 2Att_{dlp} + 2 \cdot q_kAtt_{DHP} \quad (9)$$

In the end, according to these games, the probability of an attacker breaking the security of our proposal is negligible. □

5.3. Informal Security

The proposed CM-CPPA scheme will achieve the privacy and security requirements as well as it will be proven that the proposed scheme is resistant to various attacks by the following steps.

- Privacy (identity-anonymity): In this work, the participating registered vehicle $V_i$ transmits the message-tuple $[PID_{vi}, M_i, T_{vi}, \sigma_{vi}]$ to nearby others. The true identity of vehicle $TID_{vi}$ is hidden to the message-tuple by $PID_{vi} = TID_{vi} \oplus h(s|T_{vi})$, where $s$ is the private key of the system and $T_{vi}$ is the current timestamp. During the offline registration phase (Section 4.2), once the true identity of the vehicle $TID_{vi}$ is submitted by the driver, the TA saves it to the vehicle registration list. Moreover, when the message-tuple $[PID_{vi}, M_i, T_{vi}, \sigma_{vi}]$ is captured by a third party, there is no
information about the identity of vehicle $TID_{vi}$. Therefore, the identity of the vehicle $TID_{vi}$ is the only known by the participating registered vehicle $V_i$ and the TA. So, this work achieves the privacy (identity-anonymity) requirement in 5G-enabled vehicular networks.

- **Message Authentication and Integrity:** In the proposed CM-CPPA scheme, the message-tuple $\{PID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ is included as a sophisticated signature $\sigma_{vi} = T_{SM_{vi}}(SK_{vi}) \mod P$, where $SM_{vi} = h(M_i || PID_{vi} || T_{vi})$, $SK_{vi} = T_{PID_{vi}, s}(x) \mod P$ and $PID_{vi} = TID_{vi} \oplus h(s || T_{vi})$ (Section 4.3). Based on the complexity of DLP associated with the chaotic map, the malicious vehicle $(V_m)$ cannot find/retrieve the private key of the system $s$ such that $T_{vi}(x) \equiv y$ for two given parts $x$ and $y$. Therefore, the verifier $V_j$ can confirm the authenticity and integrity of message-tuple $\{PID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ sent from vehicle $V_i$ by checking whether equation $T_{PID_{vi}}(\sigma_{vi}) \equiv T_{PID_{vi}, SM_{vi}}(SK_{vi})$ holds (Section 4.4). For instance, after capturing the message-tuple $\{PID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ sent from $V_i$, a malicious vehicle $(V_m)$ modifies/changes the safety-related message $M_i$ to a bogus message $M'_i$ and then sends the altered false message-tuple $\{PID_{vi}, M'_i, T_{vi}, \sigma_{vi}\}$ into 5G-enabled vehicular networks. The verifier $V_j$ confirms the authenticity and integrity of the altered false message-tuple $\{PID_{vi}, M'_i, T_{vi}, \sigma_{vi}\}$ by checking whether Equation (4) holds. If it holds, then the proposed CM-CPPA scheme achieves the message authenticity and integrity requirements.

- **Traceability:** In the proposed CM-CPPA scheme, the TA is responsible to register the vehicle based on an unique true identity of vehicle $TID_{vi}$ in the offline registration phase (Section 4.2). Furthermore, there is no publicly available information with respect to the true identity of vehicle $TID_{vi}$ on the message-tuple $\{PID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$, where $PID_{vi} = TID_{vi} \oplus h(s || T_{vi})$. Therefore, the TA has the capability to retrieve the true identity of vehicle $TID_{vi}$ from a pseudonym-ID $PID_{vi} = TID_{vi} \oplus h(s || T_{vi})$ included on the message-tuple $\{PID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ by executing $TID_{vi} = PID_{vi} \oplus h(s || T_{vi})$ since TA has its private key $s$ and obtained timestamp $T_{vi}$. Thus, this work achieves the traceability requirement.

- **Unlinkability:** In the proposed CM-CPPA scheme, the vehicle $V_i$ generates a new pseudonym-ID $PID^{new}_{vi} = TID_{vi} \oplus h(s || T^{new}_{vi})$ to each message generation process, where $T^{new}_{vi}$ is the new current timestamp. According to the chaotic map-based hash function $h()$, the result will change from the various initial input. Therefore, the adversary cannot link two or more message-tuples $\{PID^{new1}_{vi}, M^{new1}_i, T^{new1}_{vi}, \sigma^{new1}_{vi}\}$, $\{PID^{new2}_{vi}, M^{new2}_i, T^{new2}_{vi}, \sigma^{new2}_{vi}\}$ sent from the same sender (vehicle $V_i$). Thus, the proposed CM-CPPA scheme achieves the unlinkability requirement.

- **Resistance to modification attack:** The main malicious task of the modification attack is to launch a modified safety-related message $M_i$ to falsify the message $M'_i$ and then broadcast the altered false message-tuple $\{PID_{vi}, M'_i, T_{vi}, \sigma_{vi}\}$ in 5G-enabled vehicular networks. As a result, the entire the system will be insecure. To resist the modification attack, the verifier $V_j$ in the proposed CM-CPPA scheme can distinguish any alteration in $\{PID_{vi}, M'_i, T_{vi}, \sigma_{vi}\}$ by checking whether equation $T_{PID_{vi}}(\sigma_{vi}) \equiv T_{PID_{vi}, SM_{vi}}(SK_{vi})$ holds. If it holds, then the receiver $V_j$ accepts the message $M_i$; otherwise, it will be discarded. Hence, the proposed CM-CPPA scheme successfully withstands the modification attack.

- **Resistance to impersonation attack:** The main malicious task of an impersonation attack is to impersonate a forged message signature $\sigma_{vi}'$ as participating registered vehicle and then broadcast the forged message-tuple $\{PID_{vi}, M'_i, T_{vi}, \sigma_{vi}'\}$ in vehicular communication relying on 5G technology. Furthermore, the attacker must initially obtain/retrieve the identity of vehicle $TID_{vi}$ and the private key of the system $s$ to impersonate a legitimate vehicle. Thus, in this work, vehicle $V_i$ hides its $TID_{vi}$ into a pseudonym-ID $PID_{vi} = TID_{vi} \oplus h(s || T_{vi})$ and the private key of the system $s$ is stored in the TPD of the participating registered vehicle $V_i$. According to DLP of the chaotic
map, the adversary cannot find the private key of the system. Thus, the proposed CM-CPPA scheme successfully withstands the impersonation attack.

- Resistance to replay attack: The main malicious task of replay attack is to replay the previously generated message-tuple \( \{\text{PID}_{vi}, M_i, T_{vi}, \sigma_{vi}\} \) sent from a participating registered vehicle \( V_i \) to disturb the 5G-enabled vehicular networks. However, in this work, a timestamp \( T_{vi} \) is contained in the message-tuple \( \{\text{PID}_{vi}, M_i, T_{vi}, \sigma_{vi}\} \), where \( \sigma_{vi} = T_{SM_{vi}}(SK_{vi}) \mod P \) and \( SM_{vi} = h(M_i || \text{PID}_{vi} || T_{vi}) \). The freshness timestamp is issued by the vehicle \( V_i \) during the message generation process. Once receiving the message-tuple \( \{\text{PID}_{vi}, M_i, T_{vi}, \sigma_{vi}\} \), the verifier \( V_j \) initially checks the freshness of the timestamp to continue the verification process. Otherwise, the message will be discarded immediately. Thus, the proposed CM-CPPA scheme successfully withstands the replay attack.

- Resistance to Man-In-The-Middle (MITM) Attack: The main malicious task of MITM attack is to intercept the participating registered sender \( V_i \) and receiver \( V_j \). However, in the proposed CM-CPPA scheme, mutual authentication among nodes is executed. Furthermore, by using the AVISPA tool (Section 5.1), this work is secure against high control attackers (Dolev–Yao model) over the system. Thus, the proposed CM-CPPA scheme successfully resists the MITM attack in 5G-enabled vehicular networks.

6. Performance Evaluation

In this section, we analyze and compare the performance of the proposed CM-CPPA scheme with the three most recent schemes based on BP and EC operations.

6.1. Computation Overhead Analysis and Comparison

In this section, we analyze CPPA schemes by comparing the overhead of computation of our proposal and the existing schemes for 5G-enabled vehicular networks. For a fair comparison, some cryptography operations about the running cost are as follows.

- \( T_{pair-bp} \): the running cost of the BP operation \( \tilde{e}(S, T) \), where \( S, T \in G_1 \).
- \( T_{ptm} \): the running cost of a Point-to-Map hashing operation for the BP in \( G_1 \).
- \( T_{mul-ec} \): the running cost of operation with regards to a scale multiplication \( x.P \) for the EC, where \( x \in Z_q^* \) and \( P \in G \).
- \( T_{chev} \): the running cost of Chebyshev’s polynomial mapping operation.
- \( T_{h-chev} \): the running cost of the chaotic map hashing operations.

In this paper, negligible operations such as XOR and concatenation are not considered, and only the most significant operations are included. The hardware specification of the Windows 10 operating system contains an Intel i5-3570 processor with 16.0 gigabytes of memory and a 3.40 GHz clock frequency. The running cost of the above cryptographic operations is tabulated in Table 1.

| Cryptography Operation | Running Cost (ms) |
|------------------------|------------------|
| \( T_{pair-bp} \)      | 1.537            |
| \( T_{ptm} \)          | 0.937            |
| \( T_{mul-ec} \)       | 0.715            |
| \( T_{chev} \)         | 0.341            |
| \( T_{h-chev} \)       | 0.061            |

The existing schemes applied ECC and bilinear pairing operations to generate/sign messages and verify the validity and authenticity of the signature. These operations are considered time-consuming and complicated operations. According to Table 1, we can observe that the running costs of bilinear pair operation and scalar multiplication operation are 1.537 ms and 0.715 ms, respectively. In contrast, the running cost of the chaotic polyno-
mial map for our work is 0.341 ms to generate/sign messages and verify the validity and authenticity of signatures for 5G-enabled vehicular networks. The percentage improvement for the running cost of chaotic polynomial map over bilinear pair and elliptic curve are about \( \frac{1.537 - 0.341}{0.715 - 0.341} \approx 77.81\% \) and \( \frac{0.715 - 0.341}{0.715} \approx 52.31\% \), respectively.

This paper shows the detailed analysis of the Pournaghi et al. [30], Zhang et al. [41], Cui et al. [42] schemes and the proposed CM-CPPA scheme. The comparisons of computation Overhead for message signing and message verification steps are tabulated in Table 2.

| Schemes          | Message Signing       | Message Verification | Operations Based |
|------------------|-----------------------|----------------------|------------------|
| Pournaghi et al. [30] | 1\( T_{pair\_bp} + 1T_{ptm} \approx 2.474 \text{ ms} \) | 3\( T_{pair\_bp} + 1T_{ptm} \approx 5.548 \text{ ms} \) | Bilinear Pair |
| Zhang et al. [41]  | 3\( T_{mul\_ec} \approx 2.145 \text{ ms} \) | 2\( T_{mul\_ec} \approx 1.43 \text{ ms} \) | Elliptic Curve |
| Cui et al. [42]   | 2\( T_{chev} + 2T_{h\_chec} \approx 0.804 \text{ ms} \) | 3\( T_{chev} + 1T_{h\_chec} \approx 1.084 \text{ ms} \) | Chaotic Map |
| CM-CPPA           |                       |                      |                  |

For the message signing step of the Pournaghi et al. scheme [30], the signer requires to run one the BP operation and one Point-to-Map hashing operation for the BP. Hence, the running cost of the step is 1\( T_{pair\_bp} + 1T_{ptm} \approx 2.474 \text{ ms} \). For the message verification step of the Pournaghi et al. scheme [30], the verifier requires to execute three BP operations and one Point-to-Map hashing operation for the BP. Hence, the running cost of the step is 3\( T_{pair\_bp} + 1T_{ptm} \approx 5.548 \text{ ms} \).

For the message signing step of the Zhang et al. scheme [41], the vehicle requires to run three scale multiplication operations for the EC. Hence, the running cost of the step is 3\( T_{mul\_ec} \approx 2.145 \text{ ms} \). For the message verification step of the Zhang et al. scheme [41], the verifier requires to run two-scale multiplication operations for the EC. Hence, the running cost of the step is 2\( T_{mul\_ec} \approx 1.43 \text{ ms} \).

For both the message signing step and message verification step of the Cui et al. scheme [42], the vehicle and verifier require to run three scale multiplication operations for the EC. Hence, the running cost of the message signing step and message verification step are 3\( T_{mul\_ec} \approx 2.145 \text{ ms} \) and 3\( T_{mul\_ec} \approx 2.145 \text{ ms} \), respectively.

For the message signing step of the proposed CM-CPPA scheme, the signer requires to run two Chebyshev’s polynomial mapping operations and two chaotic map hashing operations. Hence, the running cost of the step is 2\( T_{chev} + 2T_{h\_chec} \approx 0.804 \text{ ms} \). For the message verification step of the proposed CM-CPPA scheme, the checker requires to run three Chebyshev’s polynomial mapping operations and one chaotic map hashing operation. Hence, the running cost of the step is 3\( T_{chev} + 1T_{h\_chec} \approx 1.084 \text{ ms} \).

From Table 2, it can be concluded that the proposed CM-CPPA has lower computation overhead compared to other CPPA schemes at the message signing step since the proposed CM-CPPA scheme needs only 0.804 ms while the other existing schemes of Pournaghi et al. [30], Zhang et al. [41], Cui et al. [42] need 2.474 ms, 2.145 ms, 2.145 ms, respectively. Moreover, the proposed CM-CPPA scheme has the lower computation overhead compared to other CPPA schemes at the message verification step because the proposed CM-CPPA scheme needs only 1.084 ms while the other existing schemes of Pournaghi et al. [30], Zhang et al. [41], Cui et al. [42] need 5.548 ms, 1.43 ms, 2.145 ms, respectively. Figure 5 presents the computation overhead for message signing and message verification steps, which illustrates that the proposed CM-CPPA has a lower overhead compared to the CPPA schemes.
The percentage improvement with the message signing and message verification steps of the proposed CM-CPPA scheme over the Pournaghi et al. scheme [30], Zhang et al. scheme [41] and Cui et al. scheme [42] for the total running cost. Table 3 illustrates the improvement of the proposed CM-CPPA over three CPPA schemes.

### Table 3. Improvement of the Proposed CM-CPPA Over Three CPPA schemes.

| Schemes             | Message Signing | Message Verification |
|---------------------|-----------------|----------------------|
| Pournaghi et al. [30] | 2.474−0.804 = 67.51% | 5.548−1.084 = 80.46% |
| Zhang et al. [41]    | 2.145−0.804 = 62.52% | 1.43−1.084 = 24.2%   |
| Cui et al. [42]      | 2.145−0.804 = 62.52% | 2.145−1.084 = 49.46% |

6.2. Communication Overhead Analysis and Comparison

In this section, we analyze CPPA schemes by comparing the overhead of communication for the Pournaghi et al. [30], Zhang et al. [41], Cui et al. [42] schemes and the proposed CM-CPPA scheme in vehicular communication relying on 5G technology. More precisely, in an open channel environment, the communication cost is generated between a message-tuple being broadcasted from a vehicle to others. Our work assumes that the product of a timestamp is 32 bits, the product of the hash function is 160 bits, the product of EC point is (160 + 160) = 320 bits, and the product of BP point $P = (P_x, P_y)$ is (512 + 512) = 1024 bits. The comparison of communication overhead is tabulated in Table 4.

### Table 4. Comparison of Communication Overhead.

| Schemes              | Message Tuple                        | Size of Tuple | Operations Based |
|----------------------|---------------------------------------|---------------|------------------|
| Pournaghi et al. [30] | $\{pID_i, \sigma_i, M_i, ID_{RSU}\}$ | 2528 bits     | Bilinear Pair    |
| Zhang et al. [41]    | $\{PID_j, M_j, Y_j, S_j, T_j\}$      | 832 bits      | Elliptic Curve   |
| Cui et al. [42]      | $\{PID_j, DT_{ij}, \sigma_j, D_j, T_j\}$ | 1152 bits     | Elliptic Curve   |
| CM-CPPA              | $\{PID_{vi}, M_i, T_{vi}, \sigma_{vi}\}$ | 352 bits      | Chaotic Map      |

In the Pournaghi et al. scheme [30], the vehicle broadcasts the pseudonym-ID and message signature $\{pID_i, \sigma_i, M_i, ID_{RSU}\}$ to the verifier, where $pID_i = \{pID^1_i, pID^2_i\}$, $pID^1_i$ is the BP point and $\{pID^2_i, ID_{RSU}, \sigma_i\}$ are hash functions. Hence, the communication cost of the Pournaghi et al. scheme [30] is $1024 \times 2 + 160 \times 3 = 2528$ bits.
In the scheme of Zhang et al. [41], the signer sends the pseudonym-ID and message signature \( \{ PID_i, M_i, Y_i, S_i, T_i \} \) to the verifier, where \( PID_i = \{ PID_{i,1}, PID_{i,2} \} \), \( PID_{i,1} \) is the EC point, \( \{ PID_{i,2}, Y_i, S_i \} \) are hashing functions and \( T_i \) is the timestamp. Hence, the communication cost of the Zhang et al. scheme [41] is \( 320 + 160 \times 3 + 32 = 832 \) bits.

In the scheme of Cui et al. [42], the signer sends the pseudonym-ID and message signature \( \{ PID_i, D_{T_i}, \sigma_i, D_i, T_i \} \) to the verifier, where \( PID_i = \{ PID_{i,1}, PID_{i,2} \} \), \( PID_{i,1} \) and \( D_i \) is the EC point, \( \{ PID_{i,2}, D_{T_i}, \sigma_i \} \) are hashing functions, and \( T_i \) is the timestamp. Hence, the communication cost of the Cui et al. scheme [42] is \( 320 \times 2 + 160 \times 3 + 32 = 1152 \) bits.

In the scheme of proposed CM-CPPA, the signer sends the pseudonym-ID and message signature \( \{ PID_{vi}, M_i, T_{vi}, \sigma_{vi} \} \) to the verifier, where \( PID_{vi} \) and \( \sigma_{vi} \) are a hash function and \( T_{vi} \) is the timestamp. Hence, the communication cost of the proposed CM-CPPA scheme is \( 160 \times 2 + 32 = 352 \) bits.

Figure 6 presents the communication overhead for the message tuple, which illustrates that the proposed CM-CPPA scheme has a lower overhead compared to the recent schemes based on BP and EC operations.

The percentage improvements with the communication overhead of the proposed CM-CPPA scheme over Pournaghi et al. [30], Zhang et al. [41], and Cui et al. [42] for the total message tuple cost are about \( \frac{2528 - 352}{2528} \approx 86.08\% \), \( \frac{832 - 352}{832} \approx 57.69\% \), and \( \frac{1152 - 352}{1152} \approx 69.44\% \), respectively.

7. Conclusions

This paper proposed an efficient CM-CPPA scheme that employs a Chebyshev polynomial mapping operation and a chaotic map-based hash function to secure communication in vehicular communication relying on 5G technology. A formal Security analysis is applied in our proposal for AVISPA, and the results presented in our work are safe against common attacks. On the other hand, an informal security analysis of the proposed CM-CPPA scheme shows that it achieves the security goals with regard to privacy and security properties. Ultimately, owing to the fact that the proposed CM-CPPA scheme does not employ BP and EC operations, the performance overhead of the proposed CM-CPPA scheme has better efficiency with regards to overheads of communication and computation compared to most recent existing approaches.

In future work, our proposal based on a chaotic map will be satisfied with batch verification to verify several messages simultaneously in vehicular communication relying on 5G technology. Additionally, we will investigate some related schemes that have strong assumptions to propose realistic TPD instead of ideal TPD in our work.
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: Data sharing 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. Lai, C.; Lu, R.; Zheng, D.; Shen, X. Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Netw.* 2020, 34, 37–45. [CrossRef]
2. Cheng, X.; Zhang, R.; Yang, L. Wireless toward the era of intelligent vehicles. *IEEE Internet Things J.* 2018, 6, 188–202. [CrossRef]
3. 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]
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. Alazzawi, M.A.; Al-behadili, H.A.; Srayyi 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; Springer: Berlin/Heidelberg, Germany, 2020; pp. 80–94.
6. Cheng, X.; Zhang, R.; Chen, S.; Li, J.; Yang, L.; Zhang, H. 5G enabled vehicular communications and networking. *China Commun.* 2018, 15, 3–6. [CrossRef]
7. 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. [CrossRef]
8. Prasad, K.S.V.; Hossain, E.; Bhargava, V.K. Energy efficiency in massive MIMO-based 5G networks: Opportunities and challenges. *IEEE Wirel. Commun.* 2017, 24, 86–94. [CrossRef]
9. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S. Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE Sens. J.* 2020, 21, 2422–2433. [CrossRef]
10. Cui, J.; Wei, L.; Zhang, J.; Xu, Y.; Zhong, H. An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* 2018, 20, 1621–1632. [CrossRef]
11. Hamdi, M.M.; Mustafa, A.S.; Mahd, H.F.; Abood, M.S.; Kumar, C.; Al-shareeda, M.A. Performance analysis of QoS in MANET based on IEEE 802.11 b. In *Proceedings of the 2020 IEEE International Conference for Innovation in Technology* (INOCON), Bangluru, India, 6–8 November 2020; pp. 1–5.
12. Raya, M.; Hubaux, J.P. Securing vehicular ad hoc networks. *J. Comput. Secur.* 2007, 15, 39–68. [CrossRef]
13. Cincilla, P.; Hicham, O.; Charles, B. Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios. In *Proceedings of the 2016 IEEE Vehicular Networking Conference (VNC)*, Columbus, OH, USA, 8–10 December 2016; pp. 1–8.
14. 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]
15. Joshi, A.; Gaoankar, P.; Bapat, J. A reliable and secure approach for efficient car-to-car communication in intelligent transportation systems. In *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 22–24 March 2017; pp. 1617–1620.
16. 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]
17. Thenmozi, T.; Somasundaram, R. Pseudonyms based blind signature approach for an improved secured communication at social spots in VANETS. *WIRE. Pers. Commun.* 2015, 82, 643–658. [CrossRef]
18. Rajput, U.; Abbas, F.; Oh, H. A hierarchical privacy preserving pseudonymous authentication protocol for VANET. *IEEE Access* 2016, 4, 7770–7784. [CrossRef]
Sensors 2022, 22, 5026

19. Asghar, M.; Doss, R.R.M.; Pan, L. A scalable and efficient PKI based authentication protocol for VANETs. In Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, Australia, 21–23 November 2018; pp. 1–3.

20. Förster, D.; Kargl, F.; Löhr, H. PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET). In Proceedings of the 2014 IEEE Vehicular Networking Conference (VNC), Paderborn, Germany, 3–5 December 2014; pp. 25–32.

21. 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]

22. Zhang, C.; Ho, P.H.; Tapical, J. On batch verification with group testing for vehicular communications. Wirel. Netw. 2011, 17, 1851–1865. [CrossRef]

23. Lee, C.C.; Lai, Y.M. Toward a secure batch verification with group testing for VANET. Wirel. Netw. 2013, 19, 1441–1449. [CrossRef]

24. 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.

25. Zhong, H.; Han, S.; Cui, J.; Zhang, J.; Xu, Y. Privacy-preserving authentication scheme with full aggregation in VANET. Inf. Sci. 2019, 476, 211–221. [CrossRef]

26. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. 2017, 18, 2467–2476. [CrossRef]

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. Bayat, M.; Barmsheorooy, M.; Pournaghi, S.M.; Rahimi, M.; Farjami, Y.; Aref, M.R. A new and efficient authentication scheme for vehicular ad hoc networks. J. Intell. Transp. Syst. 2020, 24, 171–183. [CrossRef]

29. Bayat, M.; Pournaghi, M.; Rahimi, M.; Barmsheorooy, M. NERA: A New and Efficient RSU based Authentication Scheme for VANETs. Wirel. Netw. 2020, 26, 3083–3098. [CrossRef]

30. Pournaghi, S.M.; Zahednejad, B.; Bayat, M.; Farjami, Y. NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. Comput. Netw. 2018, 134, 78–92. [CrossRef]

31. 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]

32. He, D.; Zeadalyy, 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]

33. Asaar, M.R.; Salmazisadeh, M.; Susilo, W.; Majidi, A. A secure and efficient authentication technique for vehicular ad-hoc networks. IEEE Trans. Veh. Technol. 2018, 67, 5409–5423. [CrossRef]

34. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Access 2021, 9, 113226–113238. [CrossRef]

35. Li, J.; Choo, K.K.R.; Zhang, W.; Kumari, S.; Rodrigues, J.J.; Khan, M.K.; Hogrefe, D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. Veh. Commun. 2018, 13, 104–113. [CrossRef]

36. Alshudukhi, J.S.; Mohammed, B.A.; Al-Mekhlafi, Z.G. Conditional Privacy-Preserving Authentication Scheme Without Using Point Multiplication Operations Based on Elliptic Curve Cryptography (ECC). IEEE Access 2020, 8, 222032–222040. [CrossRef]

37. Alazzawi, M.; Lu, H.; Yassin, A.; Chen, K. Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad hoc Network. IEEE Access 2019, 7, 71424–71435. [CrossRef]

38. Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. IEEE Trans. Depend. Secur. Comput. 2019, 18, 722–735. [CrossRef]

39. Alshudukhi, J.S.; Al-Mekhlafi, Z.G.; Mohammed, B.A. A Lightweight Authentication with Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography. IEEE Access 2021, 9, 15633–15642. [CrossRef]

40. 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]

41. Zhang, J.; Zhong, H.; Cui, J.; Tian, M.; Xu, Y.; Liu, L. Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks. IEEE Trans. Veh. Technol. 2020, 69, 7940–7954. [CrossRef]

42. 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. 2021, 23, 1247–1259. [CrossRef]

43. 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]

44. 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]