A Chebyshev polynomial-based conditional privacy-preserving authentication and group-key agreement scheme for VANET

Jiyun Yang · Jiamin Deng · Tao Xiang · Bo Tang

Received: 6 June 2021 / Accepted: 6 September 2021 / Published online: 25 October 2021
© The Author(s), under exclusive licence to Springer Nature B.V. 2021

Abstract Vehicle ad hoc network (VANET) is an open communication environment. Any user can broadcast messages, which means that it can be easily attacked by malicious users. Therefore, the authentication of vehicles is needed. In this paper, we propose a Chebyshev polynomial-based conditional privacy-preserving authentication and group-key agreement scheme for VANET. Specifically, we solve three problems in VANET: (1) we improve the effectiveness of TA by using Chebyshev polynomial to authenticate vehicles; (2) we reduce the computational burden of TA by using Chinese remainder theorem to manage group members; (3) we provide conditional privacy for users by using traceable pseudonym scheme. Theoretical and experimental results show that the proposed scheme is more efficient than most existing schemes.

Keywords Chebyshev polynomial · Conditional privacy · Chinese remainder theorem · VANET

1 Introduction

With the development of automobile industry and the improvement of economic level, the number of cars in the city continues to grow, and traffic jams and traffic accidents occur frequently. The modern intelligent transportation system (ITS) is a most promising direction to provide an efficient way to manage cars in the city [1]. As a cornerstone of ITS, vehicular ad hoc network (VANET), which is a special mobile self-organizing network, allows vehicles to communicate with each other via vehicle-to-vehicle (V2V) communications and communicate with roadside units (RSUs) via vehicle-to-infrastructure (V2I) communications. Both V2V and V2I communications are based on a dedicated short range communication (DSRC) protocol [2,3].

Among many in-vehicle applications, safety applications (such as coordinated driving, collision avoidance, lane change warning, congestion avoidance) are one of the most concerned and important applications in VANET. To implement this application, real-time traffic-related information needs to be collected and processed in a timely manner. According to the DSRC protocol, vehicles broadcast its own traffic status information, such as speed, direction and road conditions every 100 to 300 ms during driving [4]. Using this type of information, vehicles, RSUs and traffic control application centers can achieve collision avoidance and road optimization, thereby improving road safety and traffic efficiency.

However, in this form of wireless communication, VANET may receive various attacks such as malicious detection, interception, modification and replay. Message authentication is an effective defense against mali-
cious attacks, yet many types of existing authentication schemes still have various problems in terms of efficiency and security.

In this paper, we propose a conditional privacy-preserving authentication scheme based on Chebyshev chaotic mapping. Our method has following two advantages. First, it satisfies various security requirements including conditional privacy and can resist modification attack, replay attack and so on. Second, it reduces the computational overhead compared with methods based on elliptic cryptosystems or bilinear pairing and, as a result, it improves the effectiveness of authentication.

In addition, we propose a group key distribution method. Vehicles can communicate freely after authentication. Our proposed method is based on the Chinese residual theorem, which can effectively manage vehicles’ entering and leaving the group. It also ensures forward and backward security.

The main contributions of this paper are summarized as follows.

1. A novel conditional privacy-preserving authentication scheme is proposed, which is implemented using Chebyshev polynomial instead of bilinear pairing or elliptic cryptosystems with high computational cost.

2. An efficient group key distribution method based on the Chinese residual theorem is proposed for legitimate vehicles to join and leave a group, which achieves V2V communications while providing location privacy.

3. We provide a formal proof based on BAN Logic to prove the security of our scheme and conduct comprehensive analysis of the performance of our scheme in terms of computation and communication costs.

The remainder of this paper is organized as follows. Section 2 summarizes the previous works in the literature. Section 3 describes the relevant preliminary knowledge. Section 4 presents system model and security requirements. Section 5 describes our proposed scheme in detail. Section 6 analyzes the security strength of our proposed scheme. Section 7 analyzes the performance of the proposed scheme in comparison with other existing schemes. Finally, a concluding remark of the scheme is provided in Sect. 8.

2 Related works

In order to provide security, efficiency and conditional privacy for VANET, many available techniques about authentication in VANET are designed. We briefly introduce some representative related works from the following two aspects.

Authentication mechanism

In order to solve the security and privacy issues in VANET, authentication mechanism has been widely researched. Symmetric cryptography-based authentication has high computational efficiency and low communication overhead; however, the key management and key distribution are vulnerable [5], and this scheme is lack of non-repudiation property. Public-key certificates are used in public key infrastructure (PKI) as a secure and reliable method to authenticate a vehicle, which can solve the problem of symmetric encryption key distribution and ensured the security of the encryption algorithm [6]. Raya et al. [7] designed a conditional privacy-preserving model based on public key infrastructure (PKI). In this scheme, message receiver cannot track the owner of the keys. However, a large storage space is needed. OBU needs to be equipped with a large number of public and private key pairs and corresponding anonymous certificates. Moreover, it requires a large number of CRL checks. Zhang et al. [8] proposed an identity-based PKI conditional privacy authentication scheme, in which vehicles and RSUs do not need to store any certificates. However, the scheme is vulnerable to replay attacks and could not satisfy non-repudiation. He et al. [9] proposed a conditional privacy preserving authentication scheme that does not rely on bilinear pairing, greatly reducing computational overhead. Lo et al. [10] proposed an identity-based conditional privacy preserving authentication scheme that uses elliptic curves to meet privacy requirements; however, the computation cost is unsatisfactory. Vijayakumar et al. [11] proposed an efficient anonymous authentication scheme using bilinear pairing to achieve conditional privacy. However, the efficiency of this scheme is relatively low.

Chebyshev polynomials have good cryptographic properties, and Chebyshev chaotic maps are widely used in authentication and key agreement. Several studies [12,13] have proposed chaotic map-based authenticated key agreement protocols to enhance computational efficiency. Our scheme adopts Chebyshev for authentication instead of time-consuming bilin-
ear pairing operation and mapping to point operation, which not only provides conditional privacy preserving authentication and satisfies various security requirements but also improves the effectiveness of authentication.

**Group key agreement**

To provide secure channel for V2V communication in VANET, many group key management protocols are proposed. Zheng et al. [14] proposed two centralized group-key management protocols based on the Chinese remainder theorem (CRT). This method not only minimizes the overload of messages for distributing the group key but also minimizes the user side computation complexity. However, the main limitation of this approach is that computation complexity of the server side is relatively high. Vijayakumar et al. [15] proposed a Greatest Common Divisor (GCD)-based key distribution protocol which focuses on two dimensions. The first dimension deals with the reduction in computation complexity. The second dimension aims at reducing the amount of information stored in the group center and group members. However, the main limitation of this work is that the high computation complexity and high memory requirement involved in rekeying operations. Vijayakumar et al. [16] proposed a dual authentication and key management protocol that uses the Chinese remainder theorem to manage the entry and departure of vehicles within the scope of the RSU. The scheme only needs to update a small amount of information and has high computational efficiency. However, it does not implement non-repudiation. Using a pseudonym or digital signature can provide a way to implement non-repudiation authentication. Li et al. [17] proposed an anonymous conditional privacy protection authentication scheme for VANET based on message authentication code (MAC). With verifiable secret sharing (VSS), a vehicle can obtain a group key for message generation and authentication. However, it cannot implement the key update operation, and it always uses the same group key. Therefore, the forward and backward security is not guaranteed.

The group key management scheme proposed in this paper is more efficient compared with most of existing schemes. We adopt CRT-based key management scheme combined with pseudonym mechanism for vehicles to communicate in group. Vehicles use their generation key of group key $USK_i$ to get group key and then use the group key and pseudonym to send messages, which can realize non-repudiation and the forward and backward security. The computation complexity of the TA and vehicles is reduced substantially by minimizing the number of arithmetic operations taken by the TA and vehicles. Moreover, the number of key values stored by VANET users is minimized.

**3 Preliminary**

In this section, we briefly introduce some preliminaries that will be used in this paper.

3.1 Chebyshev polynomial

**Chebyshev Polynomial and Its Properties**

For integer $n$ and a variable $x \in [-1, +1]$, Chebyshev polynomial $T_n(x) : [-1, +1] \rightarrow [-1, +1]$, degree $n$, is defined as

$$T_n(x) = \begin{cases} \cos(n \cdot \arccos(x)) & \text{if } x \in [-1, 1] \\ \cos(n \theta) & \text{if } x = \cos \theta, \theta \in [0, \pi]. \end{cases}.$$ (1)

The recursive formulation is

$$T_n(x) = \begin{cases} 1 & \text{if } n = 0 \\ x & \text{if } n = 1 \\ 2xT_{n-1}(x) - T_{n-2}(x) & \text{if } n \geq 2. \end{cases}$$ (2)

**Definition 1**

One of most important property from cryptographic perspective is that the Chebyshev polynomial exhibits the semi-group property [18], as follows: $T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x))(mod\ p)$, where $n \geq 2$, $x \in (−\infty, +\infty)$, $p$ is a prime number. Obviously, $T_r(T_s(x)) \equiv T_{rs}(x) \equiv T_s(T_r(x))(mod\ p)$, where $r$ and $s$ are two positive integers, $s, r \in Z_p^*$.

**Definition 2**

Chaotic Map-based Computational Diffie–Hellman Problem (CMDHP). Given the values of $x \in (−\infty, +\infty)$, $T_r(x)mod\ p$, $T_s(x)mod\ p$ and a large prime $p$, it is intractable to compute $T_{rs}(x)mod\ p$.

3.2 Hash function based on chaotic map

Chaotic maps can be used in constructing hash function because of their properties, such as parameter-sensitivity and random-similarity. The process of algorithm is as following [19]:

**INPUT:** bit string $y$ of arbitrary length.

**OUTPUT:** 128-bit hash value.

The advantage of Chaos hash is that it can reduce basic operations. We use Chebyshev-based sequences...
to construct Hash to reduce the computational storage complexity of OBU, thereby improving the operation effectiveness.

3.3 Chinese remainder theorem

The Chinese remainder theorem states that if one knows the remainders of the Euclidean division of an integer \( n \) by several integers, then one can determine uniquely the remainder of the division of \( n \) by the product of these integers, under the condition that the divisors are pairwise coprime [14].

Let \( k_1, k_2, k_3, \ldots, k_n \) be pairwise relatively prime positive integers, and let \( a_1, a_2, a_3, \ldots, a_n \) be positive integers. Then, CRT states that the pair of congruences

\[
X \equiv a_1 \mod k_1 \\
X \equiv a_2 \mod k_2 \\
\vdots \\
X \equiv a_n \mod k_n
\]

has a unique solution mod \( \partial_g = \prod_{i=1}^{n} (k_i) \)

To compute the unique solution, the TA can compute the value as shown in Eq. (3).

\[
X = \left( \sum_{i=1}^{n} a_i \beta_i \gamma_i \right) \mod \partial_g
\]

(3)

Where, \( \beta_i = \frac{\partial_g}{k_i} \) and \( \beta_i \gamma_i \equiv 1 \mod k_i \)

4 System model and security requirements

4.1 System model

The system model of our proposed scheme is illustrated in Fig. 1. There are three main components: a TA, OBUs and RSUs.

TA: Generally, TA is considered as a highly trusted and powerful component in the proposed authentication scheme. Moreover, TA may generate and distribute group key for vehicles for secure V2V communications. Once emergencies happen, TA may track the malicious vehicles with the vehicle’s pseudonym [20,21].

RSU: RSUs are fixed infrastructures deployed on the roadside or some installations. RSU is not completely trusted. Therefore, it must be authenticated by vehicles.

OBU: Each vehicle is equipped with an on-board unit (OBU) with tamper-proof equipment. The OBU is responsible for data collection and processing. It stores secret parameters, which are used for message generation and authentication [20,21].

4.2 Security requirements

Our scheme should satisfy the following security requirements.

(1) Message authentication: Vehicle must be able to check the validity of the message before receiving it to protect it from false message attack.

(2) Conditional privacy of the vehicles: The vehicle’s real identity cannot be obtained by the adversary, but TA can get the real identity if a vehicle sends a malicious message.

(3) Forward and backward security of group-key agreement: When a vehicle leaves the group, the group key will be updated, and the left vehicle cannot compute the new group key. When a vehicle joins the group, if it wants to get previous information, it needs the previous group key. Otherwise, it cannot compute the previous key.

(4) Resistance to replay attack: The adversary captures the intermediate security transfer information and
Table 1 Notations

| Notations | Descriptions |
|-----------|--------------|
| \( r \)   | A positive integer |
| \( p \)   | An odd prime number |
| \( q \)   | A large prime number used to select random numbers, keys, etc. |
| \( GF(q) \) | A finite group |
| \( Z \)   | A finite field |
| \( f(y) \) | An odd prime number |
| \( TA \)  | The trusted authority |
| \( R_j \) | The jth road-side-unit |
| \( V_i \) | The ith vehicle |
| \( SK_{R_j} \) | Secret key of \( R_j \) |
| \( (x_{R_j}, T_{SK_{R_j}}(x_{R_j})) \) | Public key of \( R_j \) |
| \( s \)   | System private key selected by TA |
| \( sk_{r_j} \) | Secret key shared between the \( R_j \) and the TA |
| \( ID_{R_j} \) | Real identity of \( RSU_j \) |
| \( ID_{V_i} \) | Real identity of \( V_i \) |
| \( PID_{V_i} \) | The pseudonym used in the communication process of vehicle \( V_i \) |
| \( USK_i \) | The generation key of group key for each \( OBU_j \) |
| \( H(\cdot) \) | A secure cryptographic hash function |
| \( T_j(\cdot) \) | The Chebyshev polynomial |

repeats them for unauthorized access to the security key or message.

(5) Resistance to modification attack: The adversary may modify, delete, or change a specific part of the message and broadcast the modified message to achieve some selfish purposes.

5 Proposed scheme

In this section, we present our proposed scheme. We list frequently used notations in Table 1, and the overall flowchart of the scheme is briefly described in Fig. 2. We use Chebyshev chaotic map to do authentication when vehicles join the range of a RSU and provide a key agreement scheme. The detailed process of the proposed scheme will be described as follows.

5.1 System initialization phase

Prior to the deployment of the VANET, TA needs to generate some public and private parameters for the system. These parameters are preloaded into the OBU
of the vehicle at vehicle registration and sent to the RSU at RSU registration. This phase is described below.

1. TA choose a positive integer $r$ and an odd prime number $p$, then compute $q = p^r$, we assume that computations over $GF(q)$ are carried out modulo an irreducible polynomial $f(y)$ [22].
2. TA selects a random number $s \in Z$, where $s \neq 0, 1$, as system private key.
3. TA selects a secure cryptographic hash function $H$, where $H : \{0, 1\}^* \rightarrow \{0, 1\}, H$ denotes the chaotic Hash function [19].
4. TA choose random number $x, x \in GF(q), x \neq 0, 1$, compute $T_i(x)$.
5. TA share $\{T_i(x), x, H\}$ with all vehicles and RSUs during the registration of vehicles and RSUs, while keeping $s$ as its secret key.

5.2 Offline registration phase

In this stage, vehicles and RSUs need to provide the essential information like name, address, phone number, email id, etc., to TA to make offline registration.

Registration of OBU

1. Vehicle $V_i$ first approaches the TA office directly to make offline registration and provide the essential information such as name, address, phone number and email to the TA.
2. After completing the registration process, the TA provides the generation key of group key $USK_i$ for each $V_i$ and store $\{ID_{V_i}, USK_i\}$ in its tracking list database.

Registration of RSU

1. RSU $R_j$ sends privacy information (such as identity $ID_{R_j}$ and location information) to TA.
2. After checking the legitimacy of $R_j$, TA selects an integer $SK_{R_j} \in Z, SK_{R_j} \neq 0, 1$ and selects a random number $x_{R_j} \in GF(q), x_{R_j} \neq 0, 1$ and computes $T_{SK_{R_j}}(x_{R_j})$, where the $SK_{R_j}$ means the secret key of $R_j$ and $(x_{R_j}, T_{SK_{R_j}}(x_{R_j}))$ represents the public key of $R_j$.
3. TA assign $R_j$ a secret key $sk_{R_j}$ through a secure channel, where $sk_{R_j}$ is shared by $R_j$ and TA.
4. TA store $\{ID_{R_j}, sk_{R_j}\}$ in its RSU list.

5.3 Group key distribution phase

In order to get a group key for message generation and authentication within the same RSU range, vehicles must be authenticated to ensure the reliability of group key. The process is described as follows.

Authentication message generation

The process of authentication phase is shown in Fig. 3

1. Vehicles send authentication message to TA when joining in the group within the range of $R_j$.
2. $V_i$ chooses random number $x_{i,l}, l = 1, 2, 3, \ldots, k$, and publishes $T_{x_{i,l}}(x)$. $V_i$ generates pseudonym $PID_{V_i,l} = ID_{V_i}T_{x_{i,l}}(x)(mod\ f(y))$. $V_i$ selects the current timestamp $T_i$ and calculates $at_{V_i} = H(ID_{V_i} || T_i)$.
3. $V_i$ obtains $R_j$’s authentic public key $(x_{R_j}, T_{SK_{R_j}}(x_{R_j}))$ and represents the message as $M_{vi} = \{PID_{V_i,l}, at_{V_i}, T_{x_{i,l}}(x), T_i\}$. Then, it selects a random number $r \in Z, r \neq 0, 1$, computes $T_{r}(x_{R_j})$, $T_{r}SK_{R_j}(x_{R_j}) = T_{r}(T_{SK_{R_j}}(x_{R_j}))$ and sends the cipher text $C = (T_{r}(x_{R_j}), M_{vi} \cdot T_{r}SK_{R_j}(x_{R_j}) (mod\ f(y)))$ to $R_j$ through an open channel.
4. $R_j$ decrypts the message with its secret key $SK_{R_j}$ and gets the message from vehicle $V_i, R_j$ checks the validity of timestamp.
5. $R_j$ selects the current timestamp $T_{ii}$, computes $at_{R_j} = H(M_{vi} || sk_{R_j} || T_{ii})$.
6. $R_j$ sends the message $\{ID_{R_j}, at_{R_j}, M_{vi}, T_{ii}\}$ to TA via a secure channel.

Authentication message verification

In this phase, TA validates the received authentication message through $R_j$. 
(1) TA verifies the timestamp $T_{ii}$ when it receives the message $\{ID_{R_i}, at_{R_i}, M_{V_i}, T_{ii}\}$.
(2) TA calculates $at'_{R_i} = H(M_{V_i}||sk_r'||T_{ii})$. If $at'_{R_i} = at_{R_i}$, $R_j$ is a legitimate RSU.
(3) TA computes $ID_{V_i} = PID_{V_i}||T_{x_i}(X)^{-1}(mod \ f(y))$, $at'_{V_i} = H(ID_{V_i}||T_{i})$, if $at'_{V_i} = at_{V_i}$, then check whether $ID_{V_i}$ is in the tracking list, the vehicle is legal. TA get $USK_i$ to compute group key.

**Group key distribution**

In order to ensure the communication within the same RSU range, vehicles must obtain a group key for message generation and verification. In this phase, a mutual authentication process must be conducted to ensure the reliability of group key, as shown in Fig. 4. The process is described as follows.

(1) When $V_i$ enters the range of $R_j$, $R_j$ receives $V_i$’s broadcast with $PID_{V_i}$, then $R_j$ transmits the message to TA. TA can compute $ID_{V_i}$, and get $USK_i$ by tracking list $\{ID_{V_i}, USK_i\}$.
(2) TA multiplies all $USK_i$ in the range of $R_j$, $i = 1, 2, 3, \ldots, n$, $\partial g = \prod_{i=1}^{n} USK_i$. It then computes

$$x_i = \frac{\partial g}{USK_i}, \text{ where } i = 1, 2, 3, \ldots, n$$

$$x_i \times y_i \equiv 1 \mod USK_i$$

$$var_i = x_i \times y_i$$

$$\mu = \sum_{i} var_i.$$ 

(3) $V_i$ gets the group secret key from the TA via $R_j$.

(a) TA chooses a random number $kug$ as the group secret key for vehicles in the range of $R_j$.
(b) TA computes $yug = kug \times \mu$ and collects the current timestamp $T_{iii}$, then passes them to $R_j$.
(c) $R_j$ broadcast $yug$ and $T_{iii}$.
(d) $V_i$ can get $kug$ by a module division operation: $yug \mod USK_i = kug$.

**Group key updating**

When a vehicle leaves the range of RSU, the following steps are performed.

(a) TA compute $\mu' = \mu - var_i$ and choose a new group key $kug'$.
(b) Vehicles in the group update the group key by performing group key computation of the group key distribution phase.

5.4 Message generation phase

(1) $V_i$ gathers road condition and generates a message $M$ and time stamp $T_{v_i}$.
(2) $V_i$ chooses one $PID_i$, then compute $MV = H_{kug}(PID_i, M, T_{v_i})$.
(3) $V_i$ broadcast message $\{PID_i, M, T_{v_i}, MV\}$.

5.5 Message authentication phase

(1) Once receiving a message, receiver $V_j$ firstly compares the time stamp $T_{v_i}$ in the message with the current time stamp $T'_{v_i}$. If $(T'_{v_i} - T_{v_i}) \leq \Delta t$ holds, where $\Delta t$ means permissible time delay for message transmission, the message is valid. Otherwise, the message will be abandoned.
(2) $V_j$ using its own group key $kug$ to compute $MV' = H_{kug}(PID_i, M, T_{v_i})$. If $MV' = MV$, both vehicle
and message are authenticated successfully. Otherwise, the message may have been modified. In this case, receiver may send a message to TA and report the situation. The process is illustrated in Fig. 5.

5.6 Pseudonym changing

When a vehicle reaches the social spot, it can change its pseudonym $PID_{V_i,j}$ to protect its location privacy. Vehicle can choose random number $x_{i,l}, l = 1, 2, 3, \ldots, k$ and publish $T_{x_{i,l}(x)}$, then generate a different pseudonym

$$PID_{V_i,j} = ID_{V_i} T_{x_{i,l}(x)} (mod \, f(y))$$

6 Security analysis

A secure conditional privacy-preserving authentication scheme for VANET should be able to withstand various attacks mentioned in Sect. 4. In this section, we firstly demonstrate that our scheme achieves security goals by providing an authentication proof based on BAN Logic [23]. Then, we state that our scheme satisfies security requirements by informal security discussion.

6.1 Formal security proof

In this subsection, we use BAN logic [23] to formally analyze our scheme. Fundamental rules for BAN logic are listed as follows.

- R1: Message-meaning rule: $P |\equiv P \rightarrow Q, P \equiv (X)_{Y}$
- R2: Nonce-verification rule: $P |\equiv (X, Y), P |\equiv Q \rightarrow X$
- R3: Jurisdiction rule: $P |\equiv Q \rightarrow X, P |\equiv Q \equiv X$
- R4: Freshness-conjunction rule: $P |\equiv (X), P |\equiv Q \equiv X$
- R5: Session-key rule: $P |\equiv (X, Y), P |\equiv Q \rightarrow X$

There are four goals need to be proved:

- Goal 1: $TA |\equiv ID_{R_j}, at_{R_j}, M_{V_i}, T_{ii}$
- Goal 2: $R_j |\equiv PID_{V_i,j}, at_{V_i}, T_{x_{i,l}(x)}, T_i$
- Goal 3: $V_i |\equiv kug$
- Goal 4: $V_j |\equiv V_i |\equiv PID_{V_i}, M, T_{V_i}, MV$

For the formal analysis, the message exchanged among $V_i, R_j$, and $TA$ is idealized as follows.

- M1: $V_i \rightarrow R_j : \{PID_{V_i,j}, at_{V_i}, T_{x_{i,l}(x)}, T_i\}$
- M2: $R_j \rightarrow TA : \{ID_{R_j}, at_{R_j}, M_{V_i}, T_{ii}\}$
- M3: $TA \rightarrow V_i : yug$
- M4: $V_i \rightarrow V_j : \{PID_{i}, M, T_{V_i}, MV\}$

Prerequisites for the formal proof are as follows.

- A1: $R_j |\equiv R_j \leftrightarrow V_i$
- A2: $R_j |\equiv #T_{ii}$
- A3: $V_i |\equiv V_i \rightarrow PID_{V_i,j}, at_{V_i}, T_{x_{i,l}(x)}, T_i$
- A4: $TA |\equiv #T_{ii}$
- A5: $TA |\equiv R_j \Rightarrow (ID_{R_j}, sk_{R_j})$
- A6: $V_i |\equiv V_i \leftrightarrow TA$
- A7: $V_i |\equiv #T_{ii}$
- A8: $V_i |\equiv TA |\equiv USK_i$
- A9: $V_j |\equiv V_j \leftrightarrow V_i$
- A10: $V_j |\equiv #T_{V_i}$

Based on the aforementioned assumptions and logical postulates of BAN logic, we provide formal proof of our proposed scheme as follows.

By message 1, the following statement is obtained:

- S1: $R_j |\equiv V_i |\sim PID_{V_i,j}, at_{V_i}, T_{x_{i,l}(x)}, T_i$

According to S1, A1 and R1, we have:

- S2: $R_j |\equiv V_i |\equiv PID_{V_i,j}, at_{V_i}, T_{x_{i,l}(x)}, T_i$

According to S2, A2, R2 and R4, we have

- S3: $R_j |\equiv V_i |\equiv PID_{V_i,j}, at_{V_i}, T_{x_{i,l}(x)}, T_i$

According to S3, A3 and R3, we have

- S4: $R_j |\equiv PID_{V_i,j}, at_{V_i}, T_{x_{i,l}(x)}, T_i$ (Goal 2)

By message 2, the following statement is obtained
• S5: \( TA \equiv R_j \sim ID_{R_j}, at_{R_j}, M_{v_j}, T_{ii} \)
According to S5, A4, R2 and R4, we have:

• S6: \( TA \equiv R_j \sim ID_{R_j}, at_{R_j}, M_{v_j}, T_{ii} \)
According to S6, A5 and R3, we have:

• S7: \( TA \equiv ID_{R_j}, at_{R_j}, M_{v_j}, T_{ii} \)  (Goal 1)
By message 3

• S8: \( V_i \equiv kug \times \mu \)
According to S8, A6 and R1, we have:

• S9: \( V_i \equiv TA \sim kug \times \mu \)
According to S9, A7, R2 and R4, we have

• S10: \( V_i \equiv TA \equiv kug \times \mu \)
According to S10, A8, R3, we have:

• S11: \( V_i \equiv kug \)  (Goal 3)
By message 4

• S12: \( V_j \equiv PID_i, M, T_{v_j}, MV \)
By S12,A9 and R1:

• S13: \( V_j \equiv V_i \sim PID_i, M, T_{v_j}, MV \)
Based on S13, A10, R2, R4, the following equation can be gotten.

• S14: \( V_j \equiv V_i \equiv PID_i, M, T_{v_j}, MV \)  (Goal 4)

From the above-mentioned analysis, it can be seen that our protocol achieves all the goals 1-4, which guarantee a mutual authentication between nodes. Besides, it shows that vehicles can get correct group key after a mutual authentication process and vehicles within the same RSU range with same group key can communicate with each other securely.

6.2 Informal security analysis

(1) Message authentication
A vehicle must be authenticated before it gets group key to communicate with other vehicles. The sender generates a Hash value \( MV = H_{kug}(PID_i, M, T_{v_j}) \).
The receiver will check the validity of Hash by compute \( MV' \) using group key. Only when \( MV' = MV \) the message will be accepted.

(2) Conditional privacy
Preservation of the vehicle’s identity: In our scheme, vehicles communicate with each other using \( PID_{V_i,d} \), so it can protect the real identity of the vehicle in an open communication channel.
Location privacy: Our scheme provides pseudonym changing mechanism, vehicles change their \( PID \) when reaching social spots, which protects location privacy.
Traceability: If there is a malicious vehicle, TA can get the vehicle’s real identity by computing \( ID_{V_i} = PID_{V_i,j} T_{S_{x_j}}(x)(mod \ f(y)) \).

(3) Forward and backward security
When a vehicle leaves a group, the group key will be updated, and the vehicle which leaves the group is impossible to compute the new group key. Therefore, our scheme satisfies the forward security. When a vehicle joins a group, if it wants to get previous information, it needs the previous group key. Because the newly joined vehicle cannot compute the previous key, it satisfies the backward security.

(4) Replay attack
In a replay attack, malicious users repeat the previously received messages. In our scheme, we use timestamp in each message so that receivers can check the freshness of authentication messages by checking whether \( T_{v_j}' - T_{v_j} \leq \Delta t \) holds.

(5) Modification attack
An adversary may modify a message and re-broadcast it. However, we use keyed hash function \( H \) to authenticate messages. Without the group key \( kug \), it is nearly impossible to generate a valid Hash. Any modification of message \( \{ PID_i, M, T_{v_j}, MV \} \) will cause \( MV \neq H_{kug}(PID_i, M, T_{v_j}) \). The message cannot be authenticated and accepted. Therefore, our scheme can resist modification attack.

7 Performance analysis

In this section, we perform a performance analysis of our scheme from both computational overhead and communication overhead. Then, compare it with existing schemes. Our implementation is performed on a laptop consisting of an Intel Core i5-8400 CPU @ 2.80 GHz, 8G RAM, and Windows 10 OS. Some notations about execution time are defined in Table 2.

7.1 Computation cost and comparison
To give an overall analysis of computational cost, we will compute the time overhead of the following process: user authentication, group key distribution, message generation and message authentication. The execution time of related cryptographic operations are listed in Table 3.
| Table 2 | Notations | Descriptions |
|---------|-----------|--------------|
| $T_{bp}$ | The execution time of one bilinear pairing operation $\hat{e}(\hat{U}, \hat{V})$, where $U, V \in G_1$ | |
| $T_{em}$ | The execution time of one scale multiplication operation on ECC | |
| $T_{ea}$ | The execution time of one point addition operation on ECC | |
| $T_{ep}$ | The execution time of one exponentiation operation on point | |
| $T_h$ | The execution time of one hash function operation using SHA-1 | |
| $T_{ch}$ | The execution time of Chebyshev's encryption | |
| $T_{H_{key}}$ | The execution time of one keyed hash function operation using chaos map | |

| Table 3 | Execution time of several cryptographic operations |
|---------|--------------------------------------------------|
| Cryptographic operation | Execution time (ms) |
| $T_{bp}$ | 14.69 |
| $T_{em}$ | 0.715 |
| $T_{ea}$ | 0.073 |
| $T_{ep}$ | 8.12 |
| $T_h$ | 0.045 |
| $T_{ch}$ | 0.34 |
| $T_{H_{key}}$ | 0.061 |

In the scheme proposed by He et al. [9], for a vehicle to generate a message, 3 scale multiplication operations on elliptic curve $T_{em}$ and 3 hash function operations $T_h$ are required. Moreover, 3 scale multiplication operations on elliptic curve $T_{em}$, 2 point addition operations on elliptic curve $2T_{ea}$ and 2 hash function operations $T_h$ are required for a vehicle to authenticate a message.

In the scheme proposed by Azees et al. [11], 1 exponentiation operation on point $T_{ep}$ and 1 hash function operation $T_h$ are needed to generate a message. Besides, 2 bilinear pairing operations $T_{bp}$, 5 exponentiation operations on point $T_{ep}$ and 2 point addition operations on elliptic curve $T_{ea}$ are needed to authenticate a message.

The scheme of Lo et al. [10] needs 2 scale multiplication operations on elliptic curve $T_{em}$ and 2 hash function operations $T_h$ to generate a message. 3 scale multiplication operations on elliptic curve $T_{em}$, 2 point addition operations on elliptic curve $T_{ea}$ and 2 hash function operations $T_h$ to authenticate a message.

In our scheme, for a vehicle to generate a message, 4 Chebyshev encryption operations $T_{ch}$, 2 hash function operations $T_h$ and a keyed hash function operation using chaos map $T_{H_{key}}$ are required. Similarly, for a vehicle to authenticate a message, 4 Chebyshev encryption operations $T_{ch}$, 2 hash function operations $T_h$ and a keyed hash function operation using chaos map $T_{H_{key}}$ are required.

Table 4 lists the comparison of the computation cost between several related schemes and our proposed scheme. It can be seen from Table 4 that the computational cost of the proposed scheme is superior to other schemes.

### 7.2 Communication overhead

In this part, we compare the communication overhead of the proposed scheme with several existing schemes.

We assume that the sizes of the elements in $G_1$ and $G$ are 128 bytes and 40 bytes, respectively. In addition, let the output of a hash function and the size of the time stamp are 20 bytes and 4 bytes, respectively. Moreover, we assume that the origin messages are included in the finite field $\mathbb{Z}_p^*$ and have a size of 20 bytes.

We focus on the analysis of the communication overhead in the following three processes: authentication message generation, authentication message verification, and group-key generation. The communication overhead of several schemes is listed in Table 5.

In the scheme proposed by Azees et al. [11], vehicles send messages as $(M || \text{sig} || Y_k || \text{Cert}_k)$, where $\text{Cert}_k = \{Y_k || E_i || D1D_{u_i} || \gamma_u || \gamma_v || c || \lambda || \sigma_1 || \sigma_2 || \gamma_k \} \in G_1$, $M, \lambda, \sigma_1, \sigma_2 \in \mathbb{Z}_p^*$.
Z_0^*,c is a hash operation result. Therefore, the communication overhead is \( 7 \times 128 + 5 \times 20 = 996 \) bytes.

The authentication message in the scheme of Lo et al. [10] is \( \{ PID_{i,k}, M_i, t_t, K_i, R_t, V_i \} \), where \( PID_{i,k} = \{ AID_{i,1}, AID_{i,2} \}, \{ AID_{i,1}, K_i, R_t \} \in G \) and \( \{ AID_{i,2}, V_i \} \in Z_0^* \). Hence, the communication overhead is \( 40 \times 3 + 20 \times 3 + 4 = 184 \) bytes.

In our scheme, the authentication message is \( \{ PID_{i}, M, T_i, MV \} \), \( MV = H_{kug}(PID_{i}, M, T_i) \). Therefore, the total communication overhead is \( 40 + 20 + 20 + 4 = 84 \) bytes. We can see that the overall communication overhead of our solution is relatively low.

### 8 Conclusion

In this paper, we have proposed a high-efficient authentication and group-key agreement scheme for VANET. The proposed scheme uses Chebyshev chaotic mapping instead of the time-consuming elliptic curve and bilinear pairing technique to do authentication, which increases the efficiency. While ensuring security, the overall computation and communication overhead are reduced. Moreover, our solution contains a group key distribution scheme that allows group members to access the group key while providing forward and backward security. Meanwhile, location privacy is provided by adopting pseudonym changing at social spot strategy.

### Acknowledgements

The work was funded by the technological innovation and application projects of Chongqing (Grant No.cstc2019jsxmX0077).

### Data Availability

All data generated or analyzed during this study are included in this published article.

### Declarations

**Conflicts of interest** The authors declare that they have no conflict of interest.

### References

1. Shen, X., Cheng, X., Yang, L., Zhang, R., Jiao, B.: Data dissemination in vanets: a scheduling approach. IEEE Trans. Intell. Transp. Syst. **15**(5), 2213–2223 (2014)
2. Commission, F.C., et al.: Amendment of the commission’s rules regarding dedicated short-range communication service in the 5.850-5.925 ghz band. FCC, Washington, DC, USA, Tech. Rep. FCC pp. 02–302 (2002)
3. Jiang, D., Delgrossi, L.: Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In: VTC Spring 2008-IEEE Vehicular Technology Conference, pp. 2036–2040. IEEE (2008)
4. Liu, Y., Wang, L., Chen, H.H.: Message authentication using proxy vehicles in vehicular ad hoc networks. IEEE Trans. Vehicul Technol. **64**(8), 3697–3710 (2014)
5. Ye, G., Jiao, K., Huang, X.: Quantum logistic image encryption algorithm based on sha-3 and rsa. Nonlinear Dyn. (2021). [https://doi.org/10.1007/s11071-021-06422-2](https://doi.org/10.1007/s11071-021-06422-2)
6. Ye, G., Jiao, K., Wu, H., Pan, C., Huang, X.: An asymmetric image encryption algorithm based on a fractional-order chaotic system and the rsa public-key cryptosystem. Int. J. Bifurc. Chaos **30**, 2050233 (2020). [https://doi.org/10.1142/S0218127420502338](https://doi.org/10.1142/S0218127420502338)
7. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
8. Zhang, C., Lu, R., Lin, X., Ho, P.H., Shen, X.: An efficient identity-based batch verification scheme for vehicular sensor networks. In: IEEE INFOCOM 2008-The 27th Conference on Computer Communications, pp. 246–250. IEEE (2008)
9. 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. **10**(12), 2681–2691 (2015)
10. Lo, N.W., Tsai, J.L.: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Trans. Intell. Transp. Syst. 17(5), 1319–1328 (2015)
11. 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. 18(9), 2467–2476 (2017)
12. Lai, H., Orgun, M.A., Xiao, J., Pieprzyk, J., Xue, L., Yang, Y.: Provably secure three-party key agreement protocol using chebyshev chaotic maps in the standard model. Nonlinear Dyn. 77(4), 1427–1439 (2014)
13. Lee, T.F.: Efficient three-party authenticated key agreements based on Chebyshev chaotic map-based diffie-hellman assumption. Nonlinear Dyn. 81(4), 2071–2078 (2015)
14. Zheng, X., Huang, C.T., Matthews, M.: Chinese remainder theorem based group key management. In: Proceedings of the 45th annual southeast regional conference, pp. 266–271 (2007)
15. Vijayakumar, P., Bose, S., Kannan, A.: Centralized key distribution protocol using the greatest common divisor method. Comput. Math. Appl. 65(9), 1360–1368 (2013)
16. Vijayakumar, P., Azees, M., Kannan, A., Deborah, L.J.: Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. 17(5), 1015–1028 (2016)
17. Li, X., Liu, Y., Yin, X.: An anonymous conditional privacy-preserving authentication scheme for vanets. In: 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1763–1770. IEEE (2019)
18. Zhang, L.: Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fractals 37(3), 669–674 (2008)
19. Wang, Y., Liao, X., Xiao, D., Wong, K.W.: One-way hash function construction based on 2d coupled map lattices. Inf. Sci. 178(5), 1391–1406 (2008)
20. Vijayakumar, P., Azees, M., Chang, V., Deborah, J., Balusamy, B.: Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. Cluster Comput. 20(3), 2439–2450 (2017)
21. Vijayakumar, P., Chang, V., Deborah, L.J., Balusamy, B., Shynu, P.: Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. Future Generat. Comput. Syst. 78, 943–955 (2018)
22. Lima, J.B., Panario, D., de Souza, R.C.: Public-key encryption based on Chebyshev polynomials over gf (q). Inf. Process. Lett. 111(2), 51–56 (2010)
23. Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. Proc. R. Soc. Lond. Math. Phys. Sci. 426(1871), 233–271 (1989)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.