Journal of Computers Vol. 34 No. 2, April 2023, pp. 99-112
doi: 10.53106/199115992023043402008

A Lightweight V2R Authentication Protocol Based on PUF and Chebyshev Chaotic Map

Haiyan Wang, Haibing Mu*

School of Electronic and Information Engineering, Beijing Jiao tong University,
Beijing, 100044, China
{20120114, hbmu}@bjtu.edu.cn

Received 21 June 2022; Revised 15 July 2022; Accepted 10 August 2022

Abstract. Internet of Vehicles (IoV) plays an important role in enhancing the intelligence of social transportation services. However, there are existing such as privacy leakage, computational complexity and low efficiency on V2R authentication protocols. To solve these problems, a lightweight V2R authentication protocol according to physical unclonable function (PUF) and Chebyshev chaotic map is proposed. The lightweight property of PUF in this scheme can solve the resource constraint problem of the On-Board Unit (OBU) effectively. The fuzzy extractor can correct for small variations in PUF response and improve the accuracy of data transmission. Besides, Chebyshev chaotic map with good cryptographic properties establishes a secure session key while achieving mutual authentication of V2R. Finally, simulation results show that the scheme combining PUF, chaotic map, and fuzzy extractor in this paper saves 4.7% to 49% in communication and calculation overhead comparing with existing protocols. In terms of security, our scheme can also meet the requirements well in the V2R authentication protocol for IoV.

Keywords: Internet of vehicles, physical unclonable function (PUF), Chebyshev chaotic map, mutual authentication, key agreement

1 Introduction

Internet of Vehicles (IoV) is a promising intelligent transportation solution. Vehicles to Roadside unit (V2R) and Vehicles to Vehicles (V2V) are two important communication methods [1]. In the IoV system, the car is equipped with On-Board Unit (OBU) which can communicate with Road Side Unit (RSU) for V2R communication. RSU is the key device to realize vehicle-road cooperation in IoV, and OBU and RSU can be configured according to the different scenarios and information services.

V2R communication refers to the communication between mobile vehicles and fixed roadside units. Vehicles broadcast traffic-related information (such as location, direction, speed, etc.), while roadside units can detect and sense roads, vehicles, and traffic lights quickly. The information is broadcast to the vehicles located within the coverage area of the RSU after filtering and processing. Therefore, V2R communication is of great significance to improve the reliability and security of IoV. Since IoV systems operate in wireless network typically, it is easy for malicious attackers to intercept, insert, delete and modify the transmitted information [2]. Authentication and integrity protection of messages in IoV is necessary to ensure the legitimacy of messages received by vehicles or road infrastructures. In addition, if the vehicle's identification information is leaked during communication, private information such as the vehicle's location and trajectory may be exposed, which can be exploited and compromised by attackers. The identification information of the vehicle needs to be protected to prevent attackers from identifying and tracking the vehicle [2]. Therefore, a secure mutual authentication protocol that enables authentication in integrity and privacy protection for vehicle is the most essential security goal. Besides, communication and computation overheads are also challenges in V2R authentication. Because IoT devices including OBU have limited resources, some mature encryption algorithms cannot be used directly due to excessive components or consumption. The high mobility of mobile vehicles also makes real-time generation and verification of messages difficult. So a lightweight verification and authentication protocol is necessary for a secure and efficient IoV system [3]. Therefore, the key research problem in this paper is to implement V2R mutual authentication while ensuring the lightweight property and security of the protocol.

* Corresponding Author

In recent years, researchers have proposed some solutions or systems for secure authentication on the IoV. While these efforts can meet many of the safety and efficiency requirements of the IoV, they remain vulnerable to a wide variety of performance, security, and privacy issues. To solve these problems, this paper proposes a lightweight V2R mutual authentication protocol according to PUF and Chebyshev chaotic map. In the system of this scheme, in addition to the basic entity vehicles and roadside units, a trusted authority (TA) is introduced for the management of OBU and RSU, the distribution of keys, and the storage of secret parameters. The major achievements of our paper are summarized as follows.

(1) Our scheme exploits the lightweight property of PUF to reduce the burden in the authentication process greatly and achieve true applicability to resource-constrained OBU devices.
(2) We establish session keys with forwarding security between OBU and RSU based on the semigroup nature of Chebyshev's chaotic map.
(3) Our scheme implements authentication and integrity of qualified vehicle messages and vehicle privacy protection, which can effectively resist replay, counterfeit, modification, physical and cloning attacks, with high security and privacy.
(4) The specific analysis shows that our scheme provides good security and performance with low cost.

The rest of the paper is organized as follows: Section II presents some work related to secure authentication for Telematics. Section III describes the system model of the proposed protocol, the security objectives, and the cryptographic techniques used. Section IV presents the proposed authentication scheme in detail. Section V and VI give the security and the performance analysis of the protocol, respectively. Finally, the paper is summarized in section VII.

2 Related Work

The existing IoV authentication schemes can be classified into three categories according to the cryptography used in the authentication process, which are public key infrastructure (PKI)-based schemes, identity (ID)-based schemes, and group signature-based schemes. PKI-based authentication scheme provides message authenticity and non-repudiation but suffers from high communication overhead and certificate management burden [4]. It results in huge computational overhead and affects the overall system efficiency. Although the identity-based authentication scheme can solve the shortcomings of certificate storage and verification in PKI-based schemes [5]. It also suffers from large communication overhead and a lack of flexibility and dynamism [6]. In order to protect the privacy of vehicles well, a group signature-based authentication scheme is proposed in the literature [7], but group signature verification is more complex and time-consuming than traditional signatures. And there are also problems such as reduced verification efficiency and increased communication overhead in the group signature scheme [8]. In summary, there are still different degrees of problems with the security authentication protocols of IoV that need to be solved urgently.

In recent years, with the development of mobile communication technology, there are more and more studies on privacy protection in IoV. Nowadays, many IoT devices (such as OBU and other in-vehicle devices) also have problems such as limited resources, low efficiency and security. So many scholars have also started to conduct research on communication authentication taking advantage of PUF and Chebyshev chaotic map in areas such as IoV.

PUF technology is a set of miniature delay circuits that generate an infinite number of unique and unpredictable "keys" by extracting the differences in the chip manufacturing process [9]. A PUF can be defined as a function with physical non-clonability whose input and output are a Challenge-Response Pair (CRP). The input to the physical entity is called Challenge and the output generated by the random differences in the physical entity's intrinsic structure is called Response. PUF-based authentication protocols have received a lot of attention. Scheme [10] introduces PUFs without the help of trusted third parties to achieve mutual authentication and privacy protection between V2V and V2R, which is resistant to attacks such as cloning and eavesdropping. A lightweight message authentication scheme with conditional privacy for the IoV environment uses PUF and blockchain technology to design [11]. It can provide security attributes such as message authentication, message integrity, anonymity, unlinkability, and traceability. But the handling of pseudonyms in this scheme is complex, which is a cumbersome and inefficient process. Scheme [12] combines 5G and PUF to propose a V2V anonymous authentication and key agreement protocol for IoV with lightweight properties.

Chebyshev chaotic map has good cryptographic properties, and protocols based on its theory have been widely proposed and applied in recent years. Chaos mapping-based [13] cryptography can provide an efficient and

secure way for authentication and key agreement. Scheme [14] proposes a secure and lightweight multi-server authentication scheme based on Chebyshev chaotic map and fuzzy extractor. Scheme [15] implements a group-based MTC bidirectional authentication and key negotiation protocol based on an extended Chebyshev chaotic map. It improves the authentication efficiency and significantly reduces the communication overhead of the protocol. Many existing IoV authentication protocol algorithms protect vehicle privacy while reducing authentication efficiency. Scheme [16] shows that Chebyshev polynomial operations are more computationally efficient than elliptic curve scalar multiplication operations, and authentication protocols based on the Chebyshev chaotic map have significant computational advantages. Therefore, the introduction of the Chebyshev chaotic map into the IoV authentication protocol can improve the security and efficiency of the authentication scheme. In scheme [17], a symmetric key is constructed using the semigroup property of Chebyshev polynomials, and a Chebyshev chaos mapping-based authentication scheme for IoV is proposed, which can resist multiple attacks while providing conditional privacy protection.

The V2R authentication protocol proposed in this paper combines the advantages of PUF, Chebyshev chaotic map, and fuzzy extractor techniques in order to achieve lightweight and efficient mutual authentication and key agreement. It is suitable for scenarios with limited resources of in-vehicle devices and minimizes computational and communication overheads while protecting user privacy.

3 Preliminary Knowledge

In this subsection, the system model, security objectives, and related cryptographic techniques of this scheme are presented separately.

3.1 System Model

The system model in this paper mainly consists of three entities: vehicle, RSU, and Trusted authority (TA). There are wirelessly connected among vehicles, vehicles and RSUs, and wired connection between RSUs and TAs, as shown in Fig. 1.

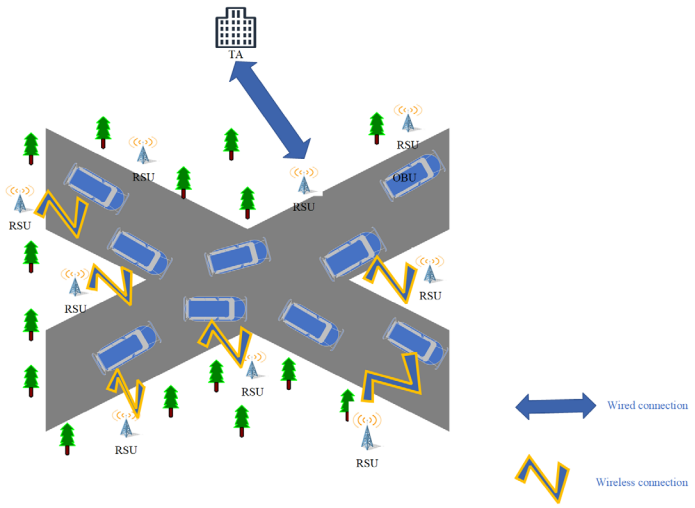

Fig. 1. System model

In this system model, there is a high probability of misbehavior in the system because the vehicles in IoV are independent individuals and have human factors. Therefore, the scheme in this paper assumes that vehicles and RSUs are semi-trusted, while only TAs are completely trusted. The specific functions of the three entities are as follows.

OBU: It is a resource-constrained device equipped on the vehicle that can perform V2X. We assume that all vehicles are equipped with PUFs on their OBUs, which are an important part of the overall authentication process.

RSU: It is the key device for vehicle-road cooperation in IoV, which collects and predicts information about the surrounding road conditions and broadcasts it to nearby vehicles and RSUs, and also interacts with TAs through a secure wired channel.

TA: It is a trusted organization such as local traffic management. It is responsible for the generation, distribution, and management of all keys and parameters in the system, and also stores the CPR generated in the PUF.

3.2 Security Objectives

We demonstrate the targeted security goals for our schemes as follows.

(1) Authenticity. The message can be verified to prevent impersonation or forgery and modification of the message by attackers. This is because wrong messages can lead to wrong decisions, which can affect the user's service experience in minor cases and cause major traffic accidents in major cases.

(2) Anonymity. The receiver of a message cannot obtain the real identity of the sender from the message. Only the trusted center stores the real identity of the vehicle, and the vehicle must hide its real ID. Otherwise, the broadcast message of the vehicle is vulnerable to eavesdropping or tracking by attackers, thus exposing the user's privacy.

(3) Traceability. When a vehicle's ID is exposed or there is a related violation, the trusted agency or traffic enforcement agency should have the ability to trace its identity from the signature of the message sent by the illegal vehicle and revoke it quickly. Besides, the offending vehicle should not deny the result of the disclosure, thus ensuring the non-repudiation of the protocol.

(4) Resistant to attacks. The authentication protocol should be able to resist eavesdropping, physical and cloning attacks, impersonation, replay, and modification to ensure the strong security of the authentication process.

(5) Forward security. RSU and OBU generate a new session key during the authentication process each time because they communicate frequently. Even if an attacker obtains your current key, it is difficult to forge a previous message or signature successfully, which can ensure the security of the session key.

3.3 PUF (Physical Unclonable Function)

PUF is an abstract one-way response function formed in an electronic device by physical excitations such as time delay, frequency, and voltage. It is called a physical unclonable function, whose description is usually expressed as a challenge-response pair (CPR), where C denotes the challenge (input) and R denotes the response (output). PUF is widely used in authentication and security keys and has good properties such as lightweight, tamper-evident, uniqueness, and other properties. Because the number and size of components to implement PUFs are small and are dependent on the differences in the physical construction of the devices generated, any tampering with PUFs produces indelible traces. For a given physical unclonable function P, constructing a contained P' physical entity makes $P = P'$ difficult [18].

3.4 Fuzzy Extractors

Since PUFs are sensitive to noise, temperature, and other operating environments, the CPRs generated by PUFs on the same device can vary slightly even under different operating environments. The fuzzy extractor [19] is divided into two parts, the generation unit, and the recovery unit, while the response (R) of the PUF can be used as the input of the generation unit to generate a key (k) and a helper data (hp). The hp can be used in the recovery unit for error correction, but it cannot be communicated in open form, otherwise, it will lead to entropy leakage. Due to the influence of the operating environment, the PUF outputs a response with certain noise differences, and the key k can be recovered by inputting R' and hp to the generation unit.

3.5 Chebyshev Chaotic Map

Chebyshev chaotic map is a special class of functions in computational mathematics that originates from the expansion polynomials of the cosine and sine functions of multiplicative angles. The extension of the Chebyshev chaotic map with the parameter x on $(-\infty,+\infty)$ can be obtained as an extended Chebyshev chaotic map with higher security [20].

Let $n \in \mathbb{Z}_q^*$, and $\forall \in (-\infty,\infty)$, p is a large prime number, the extended Chebyshev polynomial of degree n is defined as

$$T_n(x) = \cos\left(n \cdot \arccos(x)\right) (\bmod p), \tag{1}$$

where $n \geq 2$, the equivalent recursive iteration is defined as

$$T_n(x) = \left(2xT_{n-1}(x) - T_{n-2}(x)\right) (\bmod p). \tag{2}$$

The extended Chebyshev polynomial has the semi-group property, which can be used in designing key agreement protocols. Where $\forall a,b \in \mathbb{Z}_q^*$, q is a large prime number,

$$T_a\left(T_b(x)\right) (\bmod p) = T_b\left(T_a\left(x (\bmod p)\right)\right) (\bmod p) = T_{ab}(x) (\bmod p), \tag{3}$$

$$T_a(x) (\bmod p) = T_a\left(x (\bmod p)\right) (\bmod p), x \in (-\infty,+\infty) . \tag{4}$$

Also, Chebyshev polynomial can be attributed to the following two important problems. The first is discrete logarithm problem. Given n and x, it is easy to compute $y = T_n(x) (\bmod p)$. Given n and y, it is also easy to compute the value of x, but given x and y, it is very difficult to compute the value of n. Thus the problem of solving for degree n is called the discrete logarithm problem for Chebyshev chaotic map. The n is equivalent to a trapdoor that cannot be computed in regular polynomial linear time and is computationally difficult. The second is Diffie-Hellman problem. Given x, p, and the values of $T_a(x) (\bmod p)$ and $T_b(x) (\bmod p)$, it is too difficult to get the value of $T_{ab}(x) (\bmod p)$.

4 Authentication Scheme

In this protocol, we assume TA and RSU can interact with each other directly through a secure wired connection. RSU can get the stored challenge-response pairs and related key parameters in TA when required. RSU can also share part of the computation pressure for TA. RSU and OBU should authenticate each other when interacting, because the connection between them is insecure. The protocol is divided into three phases: initialization, authentication and key agreement, identity tracking and revocation, and the overall flow is shown in Fig. 2.

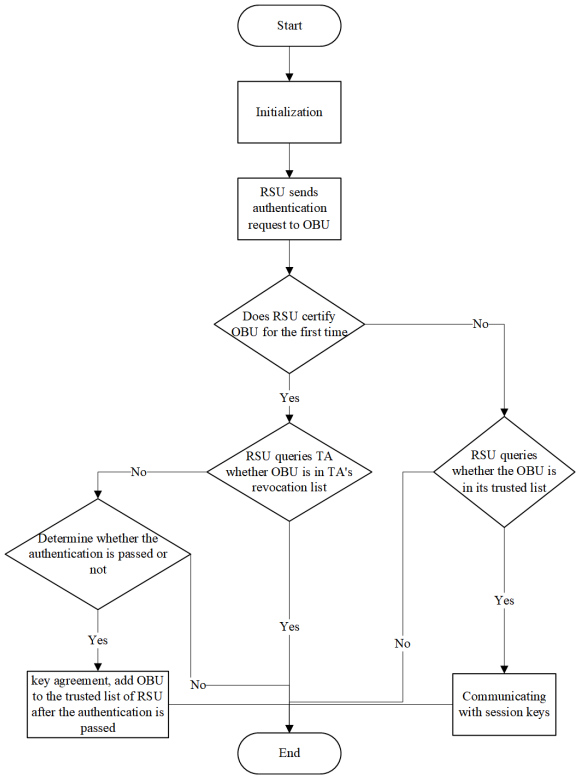

Fig. 2. Overall flow chart of the authentication protocol

The symbolic descriptions and each of the three phases in the protocol are described below.

4.1 Symbol Description

The symbols and parameters used in this protocol are shown in Table 1.

Table 1. Font symbols and parameters definition

Symbols	Description
RSU	Roadside units
TA	Trusted Authority
OBU	On-board unit
VID	Real identity of the vehicle
PID	Pseudo-identity of the vehicle
RID	Pseudo-identity of RSU
C	PUF generated challenge
R	PUF generated response
s, r_j, a, b	Random numbers
T_i , i = 1, 2, 3.....	Timestamp
$\Delta, \Delta_{ij} = T_i - T_j$	Time interval
$ENC_{key}(.)$	Symmetric encryption algorithms
$DEC_{key}(.)$	Symmetric decryption algorithms
FE.Gen(.)	Generation algorithm of fuzzy extractor
FE.Re *p*(.)	recovery algorithm of fuzzy extractor
h(.)	Hash function
$T_n(.)$	Chebyshev Chaotic Map

4.2 Initialization

The initialization phase of this protocol needs to be performed in a secure environment. In this phase, TA is responsible for the generation and assignment of the main parameters of the system. It generates the initial parameters and camouflage identification to be sent to the vehicle and RSU to complete the system initialization process. The figure and details are as follows.

(1) TA selects and exposes large prime numbers p, q, generates $s \in \mathbb{Z}_q^*$ randomly as TA's secret parameters, which can be updated periodically.

(2) OBU registration. As shown in Fig. 3, OBU sends its real identity VID and registration request to TA, TA generates and sends challenge C to OBU. Then, OBU generates the PUF output $R = PUF(C)$ and sends it to TA. Upon receiving the response R, TA calculates the pseudo-identity $PID = h(VID \| R \| s)$ and challenge $M = T_s(PID)$ of vehicle based on its own secret parameters and the received response. Moreover, TA stores $\{(C,R),PID\}$ and sends $\{PID,M\}$ to OBU. The OBU generates the PUF output $R_o = PUF(M)$, and finds the secret key k as well as the helper data hp with the help of the fuzzy generator $(k,hp) = FE.Gen(R_o)$. Finally, it sends $\{R_o,k,hp\}$ to the TA, which stores (M,R_o), k, hp.

(3) RSU registration. As shown in Fig. 3, the RSU selects $r_j \in \mathbb{Z}_q^*$ randomly as its real identity, which can be updated periodically. Then, it sends r_j to TA together with the registration request. TA generates the pseudo-identity $RID = h(r_j \| s)$ of the RSU based on r_j and its own secret parameter s after receiving the message, and sends $\{RID\}$ to the RSU.

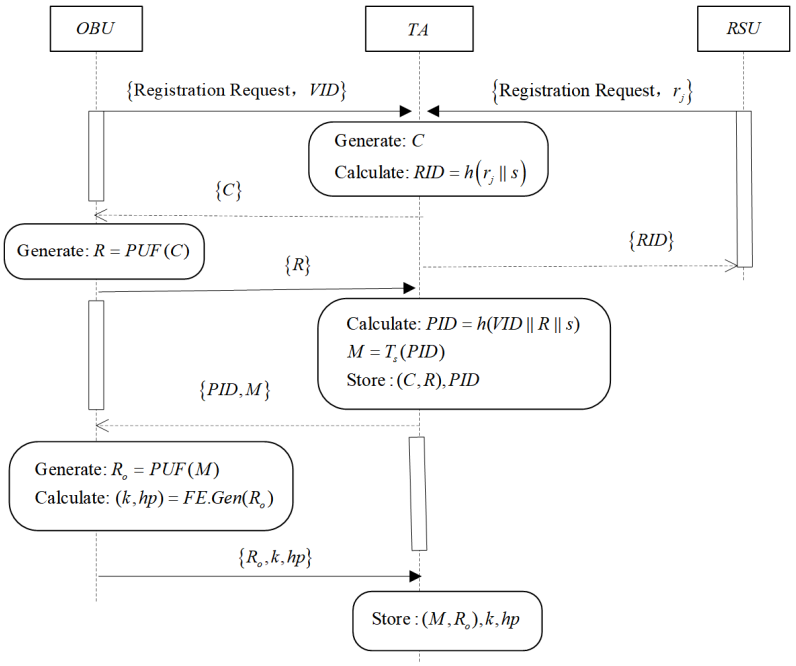

Fig. 3. Registration of OBU and RSU

4.3 Authentication and Key Agreement

This phase mainly takes OBU, RSU and TA as the main body, and after initialization, the existing parameters

they kept are as follows: $\{PID, M, k, hp\}$ for OBU, $\{RID\}$ for RSU, $\{(C, R), (M, R_o), PID, RID, s, k, hp\}$ for TA. It achieves mutual authentication between OBU and RSU using PUF, fuzzy extractor and Chebyshev chaotic map. Also, this phase generates secure session keys for frequent communication between them afterwards, as shown in Fig. 4. The process is as follows.

(1) OBU generates authentication messages: OBU first generates $a \in \mathbb{Z}_q^*$ randomly and uses its existing parameters to calculate $A = h(PID \| a)$, $P = T_a(A)$, $R_o^{'} = PUF(M)$, $B = P \oplus R_o^{'}$ to generate authentication messages $h_{o1} = h(A \| P \| B)$ and timestamp T_1. Finally, the message $\{A, P, B, h_{o1}, T_1\}$ is sent to the RSU.

(2) RSU authenticates the identity of OBU with the help of TA: After RSU receives the message from OBU, it first verifies that Δ_{21} is within time interval Δ to check the freshness of time. If it is fresh, RSU calculates $h_{o1}^{'} = h(A \| P \| B)$ based on A, P, B sent by OBU to verify the h_{o1}. If it is verified, the RSU stores *A*, *P* and sends $\{P, B\}$ to TA. TA receives and calculates $R_o^{'} = B \oplus P$, $k^{'} = FE.\mathrm{Re}\, p(R_o^{'}, hp)$. If $k^{'} = k$, then $R_o^{'}$ is uniquely generated by the OBU and the RSU authenticates the OBU successfully.

(3) After successful authentication of OBU by RSU, TA calculates $E = h(k \| hp)$ and sends $\{E\}$ to RSU.

(4) RSU generates authentication message and key parameters: After receiving the message from TA, RSU first generates $b \in \mathbb{Z}_q^*$ randomly, calculates authentication and session key parameters $N = T_b(A)$, $D = h(RID \| b)$, $N^* = D \oplus N$, $D_k = Enc_E(T_b(P))$, generates $h_{R2} = h(D \| N^* \| D_k)$ and timestamp T_3, and sends message $\{D, N^*, D_k, h_{R2}, T_3\}$ to OBU.

(5) OBU authenticates the identity of RSU, and the session key is established: After OBU receives the message sent by RSU, it first verifies that Δ_{43} is within time interval Δ to check the freshness of time. If it is fresh, OBU calculates $h_{R2}^{'} = h(D \| N^* \| D_k)$ based on D, N^*, D_k sent by RSU to verify h_{R2}. If it is verified, OBU calculates $N = N^* \oplus D$, $E^{'} = h(k \| hp)$ based on the parameters *k* and *hp* that it has, and the key is derived $T_b(P) = Dec_{E^{'}}(D_k)$. Then OBU verify $T_a(N) \stackrel{?}{=} T_b(P)$, if the equation holds, the authentication of OBU to RSU is successful and $T_a(N) = T_b(P) = T_{ab}(A)$, $T_{ab}(A)$ is the session key for communication between OBU and RSU.

4.4 Identity Tracing and Revocation

In the IoV system, even if the vehicle and RSU are authenticated before communication, there are still malicious vehicles and violations. So the tracing and revocation of the identity of malicious vehicles is necessary. TA is the only organization that can trace and revoke the identity of malicious vehicles. TA gets the information parameters $\{(C, R), (M, R_o), k, hp, PID, VID\}$ about OBU based on the $R_o^{'}$ at the time of OBU authentication. It can lock the real identity of OBU and revoke its information parameters, legal authentication and session key when violations happen. The revoked information parameters are stored in the revocation list of the TA, while the RSU has the trusted list of OBU. When RSU authenticates the identity of OBU for the first time, RSU will query its revocation list from TA before authentication, and stop the authentication immediately if OBU is in the list. If it is not in the list, RSU and OBU start mutual authentication and key agreement, and RSU add OBU to its trusted list after authentication successfully. When the OBU is added to the revocation list, the TA will broadcast a notification to the RSU to revoke its trusted record, so as to ensure the query between RSU and OBU is accurate and timely.

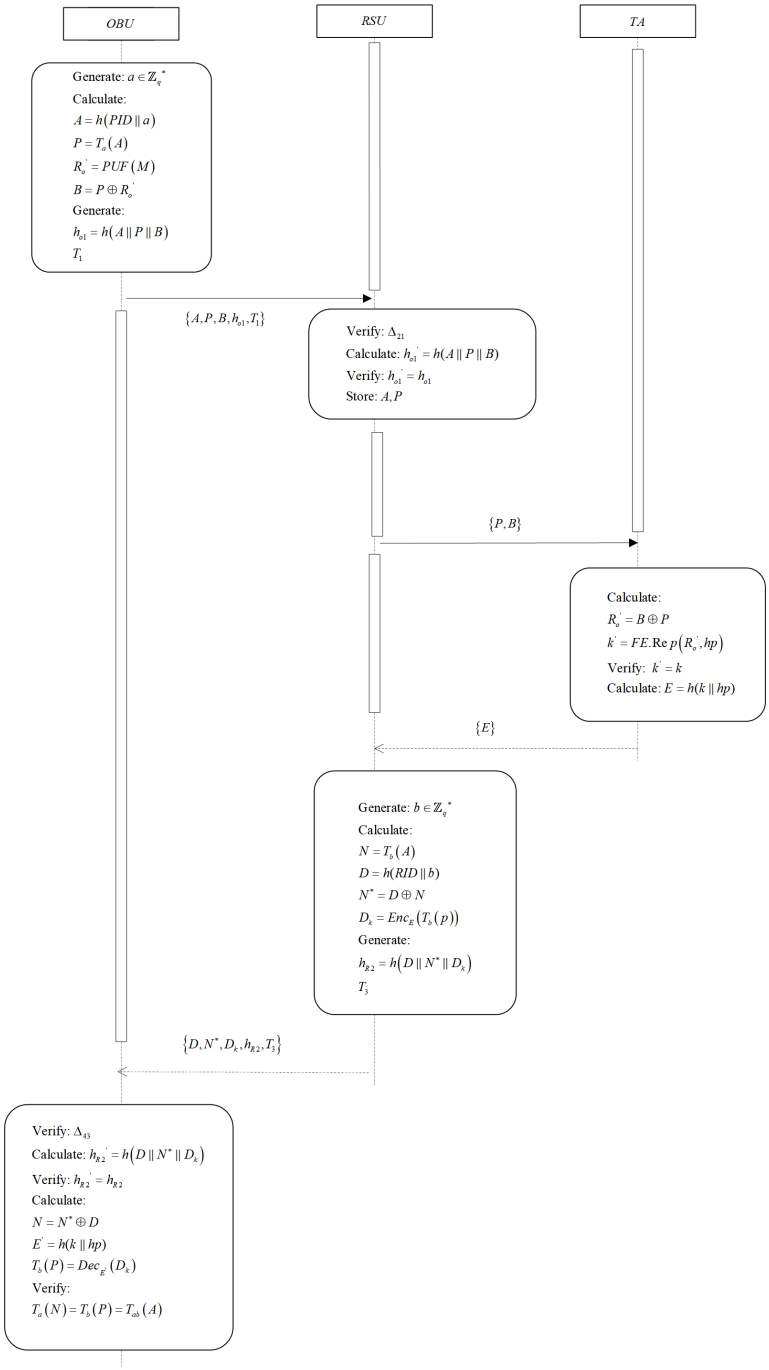

Fig. 4. Authentication and key agreement process

5 Security Analysis

5.1 Authenticity

In this scheme, the parameters in messages between OBU and RSU such as *A*, *P*, and *B* are related to *PID*, *M* and *s*. If the attacker wants to forge a valid message group successfully, he needs to forge the real identity of the vehicle VID, the secret parameter *s* of TA and random numbers *a*, *b* and other parameters. But *VID* and *s* are only

owned by TA and are not published to the public, so these parameters cannot be obtained directly and can only be constructed by means of collision.

Suppose the attacker intercepts the message $\{A, P, B, h_{o1}, T_1\}$, and to pass the RSU to OBU authentication effectively, the message tuple should be constructed within the time interval. Since message $h_{o1} = h(A \| P \| B)$, and $A = h(PID \| a)$, $P = T_a(A)$, $B = P \oplus R_o^{'}$, $R_o^{'} = PUF(M)$, and the attack which cannot directly obtain *a* and *s*, and it is also difficult to find these parameters in polynomial time, the corresponding valid message tuple cannot be constructed within time interval .

Similarly, suppose the attacker intercepts the message $\{D, N^*, D_k, h_{R2}, T_3\}$, and the composition of parameters such as D, N^*, D_k is related to the parameter *b* generated by the RSU and the parameters *k* and *hp* stored in the TA. Since none of these parameters are directly transmitted, the attacker likewise has no direct access to these secret parameters and thus cannot construct a valid message tuple within time interval. Apart from this, the rest of the message are transmitted over a secure wired channel between the RSU and the TA.

In summary, this scheme can effectively protect the authenticity and integrity of the system message. At the same time, it is also resistant to impersonation and replay attacks due to the freshness of time and the attacker does not have direct access to the secret parameters.

5.2 Anonymity

In this scheme, the real identities of vehicles and RSUs, all random secret parameters and incentive response pairs generated by vehicles are not transmitted directly. Because the corresponding pseudonyms and messages are generated for transmission after hash, exclusive OR, chaos mapping or other operations. In the whole authentication and key agreement phase, *a*, *b*, *s* are private parameters of OBU, RSU and TA respectively, which are not published to the public. According to the nature of hash function and Chebyshev chaotic map, it is difficult for an attacker to get the corresponding secret parameters even if he intercepts the transmitted message. In this protocol, the pseudonyms, secret parameters and session keys of vehicles and RSUs are changing dynamically, which is difficult for an attacker to trace. In summary, this protocol can effectively guarantee the anonymity of the system.

5.3 Traceability

As shown in 4.5, TA is the only organization that can trace and revoke the identity of a malicious legal vehicle. TA will get a parameter $R_o^{'}$ during the time of OBU authentication. Then, TA obtain the information parameters $\{(C, R), (M, R_o), k, hp, PID, VID\}$ about the OBU from the $R_o^{'}$. Next, the true identity of the OBU can be locked, and its information parameters, legal authentication and session key can also be revoked. Therefore, this scheme can achieve traceability of vehicle identity and improve the security of the system effectively.

5.4 Defends against Physical and Cloning Attacks

Each vehicle in this scheme is equipped with an embedded PUF module. It means that any physical tampering attempted by an attacker will result in the destruction of the physical characteristics of the PUF, thus changing the output of the PUF. Because the PUF is indestructible and unique, and will produce different outputs for different PUF modules even for the same input. In addition, it is known from 3.3 that PUFs are also physically unclonable, so the scheme in this paper is effective against physical and cloning attacks.

5.5 Forward Security

This scheme generates a session key for frequent communication after OBU and RSU during mutual authentication of V2R, that is, $T_a(N) = T_b(P) = T_{ab}(A)$. Assuming that the attacker intercepts N and P and knows $T_a(N)$ and $T_b(P)$, if the attacker wants to know the session key, he must find *a* or *b*. However, according to the discrete

logarithm problem of chaotic mapping, the attacker cannot find *a* and *b* based on the known $T_a(N)$ or $T_b(P)$. If the attacker wants to get $T_{ab}(A)$ directly based on $T_a(N)$ and $T_b(P)$, he will face the Diffie-Hellman problem of Chebyshev chaotic map again. Moreover, as the random numbers *a*, *b*, and *s* are updated, the session key $T_{ab}(A)$ is also updated, which makes it more difficult for the attacker to obtain the key. Therefore, the attacker cannot get the session key based on the intercepted key parameters, and this scheme can guarantee the forward security of the session key.

6 Performance Analysis and Comparison

This section gives a performance comparison of this protocol with existing IoV authentication protocols [12, 17] and identity authentication protocols based on Chebyshev Chaotic map [14, 21]. The comparisons of security properties among these protocols also show the advantages of our scheme.

We define T_{PUF}, T_h, T_c, T_s, T_m and $T_{FE.\text{Re}p}$ to represent the time for one PUF response, hash operation, Chebyshev mapping, symmetric encryption, multiplier point operation on elliptic curve and fuzzy extraction recovery, respectively. From the scheme [22], $T_c \approx 175T_h$, and from the simulation results of the scheme [23] for PUF on an MSP430 microcontroller and for other operations on a 798 MHz CPU with 256 MB RAM, the computation times for these cryptographic operations are given in Table 2 below.

Table 2. Various cryptographic operations operation time [22-23]

Cryptography operations	Execution time/*ms*
T_{PUF}	0.12
T_h	0.026
T_c	4.55
T_s	0.079
T_m	5.9
$T_{FE.\text{Re}p}$	2.85

To evaluate the communication overhead of each scheme, we assume that the size of the additive group G and the points on the elliptic curve are all 320 bits. The size of the large prime *p*, *q* and the hash, random number, identity and elements in Z_q^* are all 160 bits. The size of the chaotic map and symmetric encryption are all 192 bits. The size of challenge generated by PUF are 64 bits and the response are 128 bits. The size of the helper data and key generated by fuzzy encryption are 8 bits and 120 bits, respectively. And the size of the timestamp are 32 bits.

The comparative analysis of communication overhead and calculation overhead in authentication and key agreement phase are shown in Fig. 5 and Fig. 6, respectively.

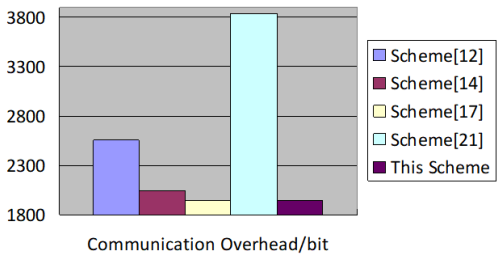

Fig. 5. Communication overhead

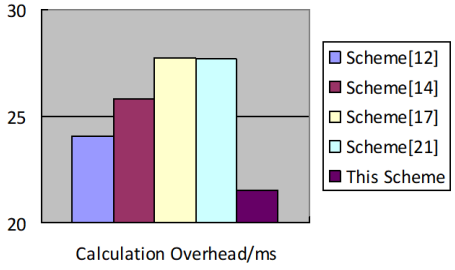

Fig. 6. Calculation overhead

The performance comparison of each scheme is shown in Table 3.

Table 3. Performance analysis

	Communication overhead/*bit*	Calculation overhead/*ms*
Scheme [12]	2552	$8T_h + 4T_m + 2T_{PUF} = 24.048$
Scheme [14]	2048	$8T_h + 5T_c + T_{FE.\mathrm{Re}p} = 25.808$
Scheme [17]	1952	$6T_c + 5T_h + 4T_s = 27.746$
Scheme [21]	3840	$6T_c + 14T_h = 27.664$
This scheme	1952	$8T_h + 4T_c + 2T_s + T_{PUF} + T_{FE.\mathrm{Re}p} = 21.536$

As shown in Table 3, in terms of communication overhead, scheme [12] has message $\{PID_1, PID_2, Q_1, MAC\}$, $\{PID_1, C_1, C_2, R_2^{'}, HLP_2, HLP_1, Q_1, H_{S2}\}$, $\{C_1, HLP_1, R_{1\_crypt}, Q_2, H_{21}\}$ and $\{H_{12}\}$ in authentication and key agreement phase, which gives a total overhead of 2552 bits. The login and authentication process in scheme [14] also generates session keys, so this phase can also be viewed as the authentication in key agreement phase. In this scheme, it gives a total overhead of 2048 bits with the messages $\{D_i, M_{i1}, M_{i2}\}$, $\{SID_j, d_i, M_{j1}, M_{j2}\}$ and $\{M_{i3}\}$. The process of a vehicle joining RSU in scheme [17] is the process of authentication and key agreement. There are messages $M_{i,j}^{\ 1} = \{P_i, C_{i,j}, x_j, tmp1\}$, $\{a_i, RID_i\}$, $\{RID_i\}$ and $M_{j,i}^{\ 2} = \{S_j, C_{j,i}, x_j, tmp2\}$ in this phase, then the total overhead is 1952 bits. In scheme [21], the messages in authentication and key agreement phase are $\{CID_{i0}, UID_j, C_1, d_1, R_1\}$, $\{CID_{i0}, CID_{j0}, C_1, d_1, R_1, C_3, d_2, R_2\}$, $\{UID_j, C_3, d_3, CID_{i1}\}$, $\{UID_i, C_1, d_4, CID_{j1}\}$, $\{d_5\}$ and $\{d_6\}$, the total overhead is 3840 bits. While there are messages $\{A, P, B, h_{o1}, tmp1\}$, $\{P, B\}$, $\{E\}$ and $\{D, N^*, D_k, h_{R2}, tmp3\}$ in our scheme, the total overhead is 1952 bits. Therefore, the communication overhead of our scheme saves 24%, 4.7% and 49% compared to the scheme [12, 14] and [21], respectively. Its communication overhead is comparable to scheme [17].

In terms of calculation overhead, as shown in Table 3, although the PUF technique is utilized in scheme [12], there are multiple elliptic curve times point operations with high overhead. The main overhead of this paper and several other schemes is the Chebyshev chaotic map operation. But this paper uses the combination of PUF and Chebyshev chaotic map and fuzzy extractor to reduce the number of Chebyshev chaotic map. Therefore, the calculation overhead of this scheme is significantly smaller than several other comparison schemes, which saves 10.4%, 16.6%, 22.4% and 22.2% compared to the scheme [12, 14, 17, 21], respectively.

In terms of security, scheme [17] implements authentication between the vehicle and the RSU using Chebyshev chaotic map. It is also assumed that both OBU and RSU are equipped with tamper-proof devices (TPDs) for long-term storage of secret parameters. However, the TPDs might be infeasible or do not exist in reality due to high security requirements [24-25]. In our scheme, we combine the TPD and PUF in OBU, which can resist physical, cloning or side-channel attacks well.

7 Conclusion

Because malicious attackers can easily intercept, insert, delete, and modify the transmitted information in V2R authentication. We propose a lightweight V2R authentication scheme based on PUF and Chebyshev chaotic map in this paper. It solves the problems such as privacy leakage, computational complexity and low efficiency of current V2R authentication protocols, and the resource limitation and poor computational capability of in-vehicle devices. The scheme introduces PUF and Chebyshev chaotic map to achieve key agreement in the authentication process. It also incorporates a fuzzy extractor to avoid the output discrepancy of the PUF response due to the influence of noise during the protocol, which ensures the correctness of the transmitted data. The performance analysis results show that this paper combines PUF, chaotic mapping and fuzzy extractor with lower computation and communication overhead than the scheme using only one or two of them. It also combines the security advantages of the three themselves, with a higher overall comprehensive performance, which can meet the requirements in the V2R authentication protocol well for IoV. The future work is going to focus on the authentication between vehicles and vehicles based on PUF and Chebyshev chaotic map. At this time, there is no RSU in the system model, only OBU and trusted authority. And the differences between V2R and V2V authentication protocol will be analyzed in detail.

References

[1] X.-T. Ma, J.-H. Zhao, C.-Y. Wang, Y.-G. Xu, V2R communication in internet of vehicles, Telecommunications Science 32(8)(2016) 21-27.

[2] L. Zhang, Q.-H. Wu, J. Domingo-Ferrer, B. Qin, C.-Y. Hu, Distributed Aggregate Privacy-Preserving Authentication in VANETs, IEEE Transactions on Intelligent Transportation Systems 18(3)(2017) 516-526.

[3] S.A. Alfadhli, S. Alresheedi, S. Lu, A. Fatani, M. Ince, ELCPH: An Efficient Lightweight Conditional Privacy-Preserving Authentication Scheme Based on Hash Function and Local Group Secrete Key for VANET, in: Proc. 2019 The World Symposium on Software Engineering, 2019.

[4] M. Raya, J.P. Hubaux, Securing vehicular ad hoc networks, Journal of computer security 15(1)(2007) 39-68.

[5] C. Zhang, R. Lu, X. Lin, P.H. Ho, X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, in: Proc. 2008 IEEE INFOCOM 2008-The 27th Conference on Computer Communications, 2008.

[6] Y.-H. Wang, Research on the Authentication Technology and Algorithm for Internet of Vehicles, [dissertation] Chongqing: Chongqing University of Posts and Telecommunications, 2017.

[7] Y.-P. Sun, Q.-L. Hu, J.-S. Su, A Distributed Key Management Scheme for the Group Signature Based on Authentication in VANETs, Computer Engineering & Science 34(7)(2012) 6-11.

[8] W.-X. Pu, A Lightweight Group-based Secure Authentication and Communication Scheme in VANETs, [dissertation] Wuhan: Wuhan University, 2019.

[9] X. Chen, Research on RFID Security Authentication Protocol based on Physical Uncloning Technology, [dissertation] Nanjing: Nanjing University of Posts and Telecommunications, 2020.

[10] B.-Y. Liu, Y. Zhang, Y.-T. Yang, Y.-F. Sun, Lightweight mutual authentication protocol based on PUF function, Computer Engineering 45(2)(2019) 38-41, 52.

[11] L. Xiong, F.-G. Li, Z.-C. Liu, Conditional Privacy-preserving Authentication Scheme Based on Blockchain for Vehicular Ad Hoc Networks, Computer Science 47(11)(2020) 55-59.

[12] W.-Y. Hou, Y. Sun, D.-W. Li, J. Cui, Z.-Y. Guan, J.-W. Liu, Anonymous Authentication and Key Agreement Protocol for 5G-V2V Based on PUF, Journal of Computer Research and Development 58(10)(2021) 2265-2277.

[13] L. Kocarev, S. Lian, Chaos-Based Cryptography: Theory, Algorithms and Applications, Springer, Germany, 2011.

[14] M. Zhang, Q.-H. Liu, J.-B. Gong, Authenticated scheme based on chaotic map and fuzzy extractor, Computer Engineering and Design 39(12)(2018) 3655-3660, 3673.

[15] P. Roychoudhury, B. Roychoudhury, D.K. Saikia, Provably secure group authentication and key agreement for machine type communication using Chebyshev's polynomial, Computer Communications 127(2018) 146-157.

[16] J. Cui, Y.-L. Wang, J. Zhang, Y. Xu, H. Zhong, Full session key agreement scheme based on chaotic map in vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 69(8)(2020) 8914-8924.

[17] J.-Y. Yang, R.-D. Yao, J. Zhou, L.-Y. Gao, Efficient authentication scheme based on Chebyshev chaotic map for VANET, Computer Engineering 47(10)(2021) 34-42, 51.

[18] Z.-N. Zhang, Y.-B. Guo, Survey of physical unclonable function, Journal of Computer Applications 32(11)(2012) 3115-3120.

[19] T.-Z. Xu, T.-C. Yang, J. Cheng, Q.-F. Shao, Design Method of SRAM-PUF Based on Error Correcting Code Fuzzy Extractor, Computer Science 43(11A)(2016) 373-376.

[20] J. Yang, D. Wang, Applying Extended Chebyshev Polynomials to Construct a Trap-Door One-Way Function in Real Field, in: Proc. 2009 First International Conference on Information Science and Engineering (ICISE), 2009.

[21] Y. Cao, Dynamic identity authentication key agreement protocol based on extended chaos mapping, Journal of Chengdu University of Technology (Science & Technology Edition) 48(4)(2021) 505-512.
[22] K. Xue, P. Hong, Security improvement on an anonymous key agreement protocol based on chaotic maps, Communications in Nonlinear Science and Numerical Simulation 17(7)(2012) 2969-2977.
[23] P. Gope, PMAKE: Privacy-aware multi-factor authenticated key establishment scheme for Advance Metering Infrastructure in smart grid, Computer Communications 152(2020) 338-344.
[24] P. Kocher, J. Jaffe, B. Jun, P. Rohatgi, Introduction to differential power analysis, Journal of Cryptographic Engineering 1(01)(2011) 5-27.
[25] B. Wang, Y. Wang, R. Chen, A practical authentication framework for VANETs, Security and Communication Networks 2019(2019).