RESEARCH ARTICLE

Zero-knowledge identity authentication for internet of vehicles: Improvement and application

Mu Han[1], **Zhikun Yin**[1], **Pengzhou Cheng**[1], **Xing Zhang**[1], **Shidian Ma**[2]*

1 School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China,
2 Automotive Engineering Research Institute Jiangsu University, Zhenjiang, China

* hanmuktz888@gmail.com

Citation: Han M, Yin Z, Cheng P, Zhang X, Ma S (2020) Zero-knowledge identity authentication for internet of vehicles: Improvement and application. PLoS ONE 15(9): e0239043. https://doi.org/10.1371/journal.pone.0239043

Editor: Xiong Li, University of Electronic Science and Technology of China, CHINA

Received: May 7, 2020

Accepted: August 30, 2020

Published: September 28, 2020

Data Availability Statement: All relevant data are within the manuscript and its Supporting Information files.

Funding: This research was supported by the Innovation Plan for Postgraduate Research of Jiangsu Province in 2014 (Grant No. KYLX1057), National Science Foundation of China (Grant No. 61902156), and Natural Science Foundation of Jiangsu Province (Grant No. BK20180860).

Competing interests: The authors have declared that no competing interests exist.

Abstract

The popularity of Internet of Vehicles (IoV) has made people's driving environment more comfortable and convenient. However, with the integration of external networks and the vehicle networks, the vulnerabilities of the Controller Area Network (CAN) are exposed, allowing attackers to remotely invade vehicle networks through external devices. Based on the remote attack model for vulnerabilities of the in-vehicle CAN, we designed an efficient and safe identity authentication scheme based on Feige-Fiat-Shamir (FFS) zero-knowledge identification scheme with extremely high soundness. We used the method of zero-one reversal and two-to-one verification to solve the problem that FFS cannot effectively resist guessing attacks. Then, we carried out a theoretical analysis of the scheme's security and evaluated it on the software and hardware platform. Finally, regarding time overhead, under the same parameters, compared with the existing scheme, the scheme can complete the authentication within 6.1ms without having to go through multiple rounds of interaction, which reduces the additional authentication delay and enables all private keys to participate in one round of authentication, thereby eliminating the possibility that a private key may not be involved in the original protocol. Regarding security and soundness, as long as private keys are not cracked, the scheme can resist guessing attacks, which is more secure than the existing scheme.

Introduction

The rise of IoV technology has not only changed the way people travel, but also made people's driving environment more and more comfortable [1]. However, the interconnection of networks between vehicles brings various information security, which makes the attack surface of the internal vehicle networks rise sharply, especially for remote attacks [2, 3]. In 2013, Toyota Prius cars were attacked by a hacker through the On-Board Diagnostic (OBD) interface and the braking systems were illegally manipulated, which caused traffic accidents [2]. In 2015, the 360 Crack team successfully cracked Build Your Dreams (BYD) and Tesla intelligent vehicles through remote and short-range attacks [4]. In the same year, Charlie Miller and Chris Valasek demonstrated the process of remotely attacking the Jeep Cherokee on-board system, including manipulation of speed, direction, brakes, and wipers [5]. In 2016, Tencent Keen Security Lab remotely reset the Bluetooth connection password of the Xiaomi Millet Nine Balancing Vehicle to achieve illegal manipulation. The following year, Tencent Keen Security Lab again found multiple high-risk vulnerabilities of security in Tesla's in-vehicle network [6]. In 2019, Tencent Cohen Lab can remotely gain the root privileges of the "Autopilot Electronic Control Unit (ECU)" module and control the steering system of the vehicle [7].

The above security issues are attributed to the lack of security protection mechanism in the traditional in-vehicle network [4]: 1) External devices have unrestricted access to in-vehicle data via wireless, Bluetooth, cellular network or OBD [8, 9]. 2) The information data of in-vehicle network are transmitted in the form of broadcast and plaintext, such as in the CAN bus. The broadcast data frame does not cover the source address and destination address [10]. Although [11–15] studied the security of in-vehicle networks to address these emerging issues, these in-vehicle security schemes focus on ensuring secure communication between ECUs with little consideration for the security issues introduced by external devices connected to the vehicle. The remote attacks on vehicles usually come from external networks or devices. If we only protect the vehicle network, such as data encryption, ECU authentication, data access control, which seems to be unable to play a decisive role, illegal devices can still inject malicious data frames into the vehicle network. Therefore, it is urgent to study the resistance to the invasion of external malicious nodes.

Contributions

Identity authentication is very important as one of the important means to prevent external intrusion. However, we also had to consider the security of the authentication protocol, because an attacker can eavesdrop on valid authentication information in the authentication protocol to fake an identity. Therefore, we adopt the zero-knowledge identity authentication method to effectively solve the problem of proof information leakage in the prover's proof process. In this paper, based on the remote attack model for vehicles, we designed an efficient and safe identity authentication scheme based on FFS zero-knowledge identification scheme with extremely high soundness, which realizes the identification of the vehicles to the external devices and solves the security threat of unauthorized access and illegal intrusion. The main contributions of this paper are presented as follows:

1. Based on the analysis of existing attack events, we proposed a common remote attack model on vehicles and conduct a security threat assessment.
2. Based on the common remote attack model, we designed an efficient and safe identity authentication scheme based on FFS zero-knowledge identification scheme with extremely high soundness. The FFS scheme is based on the Quadratic Residue (QR) difficult problem. We improved the FFS scheme so that it can be applied to the IoV scenario that requires low latency and high security. We used the method of zero-one reversal and two-to-one verification to solve the problem that FFS cannot effectively resist guessing attacks. Therefore, it can meet extremely high soundness in one iteration of authentication.
3. We constructed a security architecture in a hardware environment and performed performance evaluation. According to the evaluation results, the scheme can complete the authentication without having to go through multiple rounds of interaction, which reduces the additional authentication delay and enables all private keys to participate in one round of authentication, thereby eliminating the possibility that a private key may not be involved in the original protocol. Regarding security and soundness, as long as private keys are not

cracked, the scheme can resist guessing attacks. Therefore, the proposed scheme takes precedence over existing solutions in terms of time delay and security.

Organization

The rest of this paper is organized as follows: In Section 2, we reviewed more related work. Section 3 presented some preliminary knowledge and analysis of FFS scheme. Section 4 presented the main remote attack model for the actual vehicle and the resulting security threat assessment. Section 5 introduces our scheme. In Section 6, we conducted a theoretical analysis of the security of the proposed architecture. In Section 7, we simulated and evaluated the performance of the proposed solution. Finally, Section 8 presented the summary of this study.

Related work

Considering that the security of in-vehicle networks directly threatens the security of users' lives and property, the information security problems caused by external devices have to be solved. However, due to the low computing power of the ECU, solving the problems of vehicle network information security is still a huge challenge [1]. In order to resist forgery attacks, tampering attacks, replay attacks, and privacy leak attacks, researchers have studied many authentication schemes in the IoV or in-vehicle network [3, 12]. Research on authentication protocols based on privacy protection policies is the main method to ensure the integrity, reliability, and identity privacy of message transmission. It is also the basis for ensuring the security of information transmission in IoV. When any entity in the IoV receives relevant traffic messages, it must first pass authentication to ensure that the source of the message is reliable, the content is complete and authentic, has not been tampered with and replayed, and the identity of the user has not been leaked.

In order to solve the problem of certificate management in Public Key Infrastructure (PKI), Shamir [16] proposed identity-based cryptosystems in 1984. In this system, the identity information of each user can be used as the user's public key, such as e-mail name, phone number, ID number. The third-party trusted Public Key Generator (PKG) computes a private key based on the public key for each user and sends it to the user. Users can use the public and private keys in their hands for data encryption and digital signature operations. The cryptosystems provide data integrity mechanisms, digital envelopes, user identification, user authentication, and other technologies. On this basis, Shamir et al. [17, 18] proposed a zero-knowledge identity authentication scheme based on QR, but this scheme cannot effectively resist key guessing attacks. Kumari et al. [19] proposed an improved smart card based authentication scheme for session initiation protocol, which increases the probability of resisting key guessing attacks.

In the application scenario of IoV, Chim [20] proposed an identity-based authentication scheme, which is based on a bilinear pairing algorithm, can support batch authentication, and has low computing energy consumption. However, Horng et al. [21] believed that Chim's scheme could not resist forgery attacks and proposed a security scheme to overcome the problem of forgery attacks. However, since this scheme is based on bilinear pairing operations, its calculation time is three times that of ordinary dot multiplication operations [22]. Wang and Liu [23] proposed a certificate-based multi-level security authentication scheme that integrates all the inside and outside interfaces of the vehicles into the On Board Unit (OBU). However, in the system initialization of this scheme, a secure channel is used to transmit the symmetric key, and only the certificate is used for authentication during the two-way handshake authentication process. Therefore, the security of this solution is not high. Woo et al. [24] proposed to split the truncated MAC into the extended ID field and CRC field of the data frame, which can reduce the bus load, but it makes the data frame lack security and cannot verify the error during transmission. In addition, the scheme they proposed only had key negotiation for external devices and no identity verification, which greatly increased security risks. Li et al. [25] proposed a robust and energy-saving three-factor authentication protocol that can block the most common attacks and provide some ideal functions. The protocol reduces the power consumption and computational cost of nodes by using appropriate communication models and lightweight algorithms. Ying and NAYAK [26] proposed an anonymous lightweight authentication method based on smart card protocol, which uses low-cost encryption operations to verify the legitimacy of vehicles and data messages. From the above, these literatures use the identity-based key system in the IoV, combining the different characteristics of the IoV, to achieve the reliability and confidentiality of information transmission. Although many solutions can guarantee high security, most of them are not applicable in the scenario of fast connection authentication of the IoV. Therefore, it is of great research value to design a safe and effective authentication scheme for the connected vehicle application scenario.

Background

Quadratic residue problem

Definition 1 [27, 28]: Let n be a positive integer. If the congruence $x^2 \equiv a$ mod n have a solution and gcd $(a, n) = 1$, then a is called the quadratic residue of modulo n, where gcd means taking the greatest common divisor. Otherwise, a is called the quadratic non-residue of the module n.

The important conclusion about quadratic residue in number theory is given here directly: if $n = p * q$, where p and q are two prime numbers, a is the quadratic residue of modulo n if and only if formula (1) holds, where the symbol () in formula (1) is the Jacobi symbol. Based on this, the definitions of quadratic residue and pseudo-quadratic residue are given, as defined 2.

$$\left(\frac{a}{p}\right) = \left(\frac{a}{1}\right) = 1 \tag{1}$$

Definition 2 [27, 28]: $QR(n)$ represents the set of quadratic residues of all modules n and $Q\tilde{R}(n)$ represents the set of pseudo quadratic residues of all modules n, and their definitions are as follows:

$$QR(n) = \left\{x \in Z_n : \left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = 1\right\} \tag{2}$$

$$Q\tilde{R}(n) = \left\{x \in Z_n : \left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1\right\} \tag{3}$$

QR problem: from Definition 2 and Jacobi symbol correlation operation, it can be known that for any $x \epsilon QR(n)$, there is formula (4); if formula (5) holds, then $x \epsilon QR(n)$ or $x \in Q\tilde{R}(n)$. Only by knowing the values of p and q can you determine which set x belongs to. In other words, given a composite number n and an x ($x \epsilon Z_n$), x is determined to be the quadratic residue of the modulus n, where n is obtained by multiplying two large prime numbers p and q.

QR hypothesis: Let F_{QR} be a polynomial probability time efficient algorithm for solving QR problem. The $Adv_{QR} = Prob[F_{QR}(n,x) = yes\ (x \epsilon QR(n))]$ is used to represent the probability that the algorithm F_{QR} solves the QR problem in polynomial time. If and only if there is no polynomial probability time algorithm which can solve the QR problem, the QR hypothesis is true (i.e., Adv_{QR} is negligible).

$$\left(\frac{x}{n}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right) = 1 \tag{4}$$

$$\left(\frac{x}{n}\right) = 1 \tag{5}$$

Analysis of feige-fiat-shamir identification scheme

The Feige-Fiat-Shamir [17, 29, 30] identification scheme [30] is derived from the Fiat-Shamir [18] identification scheme, which is based on the intractability of computing square roots modulo n [29]. The parallel interactive mode's process of the FFS identification scheme [31, 32] is shown in Fig 1.

Attackers can use public keys to forge a promise to spoof. The forgery process is shown in Fig 2. FFS identification scheme is provably secure against chosen message attack in the following sense: provided that factoring n is difficult, the best attack has a probability 2^{-kt} of successful impersonation [29]. Choosing k and t such that $k^*t = 20$ allows a 1 in a million chance of impersonation, which suffices in the case that an identification attempt requires a personal appearance by a would-be impersonator [29]. Specific parameter choices might be, for security 2^{-20}: k = 5, t = 4. At present, the value of the number of bits of the parameter n requires more than 1024 bits in terms of calculation security [33]. Dhanya and Megha [33] Proposed an improved parallel interactive Feige-Fiat-Shamir identification scheme with almost zero soundness error and complete zero-knowledge. If the FFS authentication scheme is applied to an actual network communication environment, the security parameters need to be weighed. However, because of the high requirements for communication time in some application environments, these identification schemes seem not so suitable. To make identification schemes like FFS applicable to demanding application environments, further improvements are needed, which is also worth studying.

Provable security

In 1984, Goldwasser and Mlicali [34] proposed provable security, which is an axiomatic research method and a new proof of security. The following security model will be used in section VI. Let *A* be the attacker and *C* be the challenger.

Initialization phase: *C* initializes the system and sends the public system parameters to *A*.

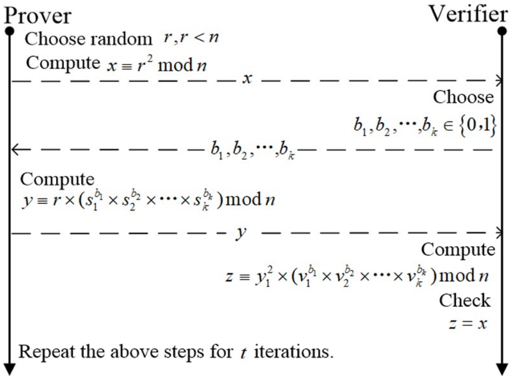
Prover
Verifier
Choose random $r, r < n$
Compute $x \equiv r^2 \bmod n$
x
Choose
$b_1, b_2, \cdots, b_k \in \{0,1\}$
$b_1, b_2, \cdots, b_k$
Compute
$y \equiv r \times (s_1^{b_1} \times s_2^{b_2} \times \cdots \times s_k^{b_k}) \bmod n$
y
Compute
$z \equiv y_1^2 \times (v_1^{b_1} \times v_2^{b_2} \times \cdots \times v_k^{b_k}) \bmod n$
Check
$z = x$
Repeat the above steps for t iterations.

Fig 1. FFS identification scheme.

https://doi.org/10.1371/journal.pone.0239043.g001

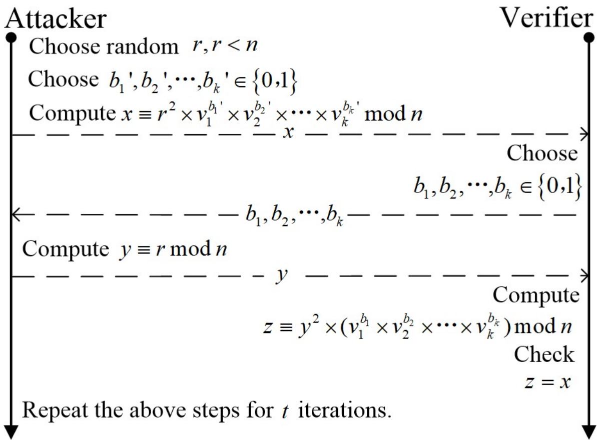
Attacker
Verifier
Choose random $r, r < n$
Choose $b_1', b_2', \cdots, b_k' \in \{0,1\}$
Compute $x \equiv r^2 \times v_1^{b_1'} \times v_2^{b_2'} \times \cdots \times v_k^{b_k'} \bmod n$
x
Choose
$b_1, b_2, \cdots, b_k \in \{0,1\}$
$b_1, b_2, \cdots, b_k$
Compute $y \equiv r \bmod n$
y
Compute
$z \equiv y^2 \times (v_1^{b_1} \times v_2^{b_2} \times \cdots \times v_k^{b_k}) \bmod n$
Check
$z = x$
Repeat the above steps for t iterations.

Fig 2. The attacker guesses b_i' in advance and hides the corresponding public key $v_i^{b_i'}$ in the promise *x*. Then, ignore the received b_i, and directly send the random number *r* as the response *y* to the verifier. Finally, if b_i' are equal to b_i, the forgery is successful.

https://doi.org/10.1371/journal.pone.0239043.g002

Phase 1: *A* makes a query for C (i.e., *A* sends ciphertext *c* to *C*, and *C* decrypts ciphertext c and sends the decrypted plaintext m_b to *A*).

Challenge: *A* outputs two equal-length plaintext messages m_0 and m_1, and then receives m_b ciphertext c_b from *C*, where $b \epsilon \{0,1\}$.

Phase 2: *A* continues to repeat the process of Phase 1.

Guess: *A* outputs a random value $b' \epsilon \{0,1\}$, and if $b' = \mathrm{b}$, *A* challenges successfully.

If the advantage of attacker A’s successful attack in the probability polynomial time is negligible, the designed solution is safe.

Attack model and security threat assessment

Attack model

In reality, the attacker is more inclined to conduct remote attacks on vehicles. Vulnerabilities of in-vehicle networks include weak access control mechanisms, plaintext transmission and no identity authentication. If an attacker wants to control the vehicle through vulnerabilities of in-vehicle networks, he can pretend to be a legitimate external device, such as mobile phones and headphones, to deceive the vehicle communication unit, such as navigation systems and entertainment information systems. It is challenging to attack the in-vehicle CAN network through remote attacks. The attacker needs to first break through the vehicle communication unit, such as OBU and telematics. After successfully controlling the in-vehicle communication unit, they can steal and analyze the data in the CAN network, then fake the legitimate data frames, and inject them into the CAN network, which will cause great harm to the in-vehicle key ECUs [35]. Fig 3 presents the eight common attack surfaces and their attack processes. If the attacker is around the car, he can invade from the following attack surfaces including Wi-Fi, Cellular network, Car virtual key, Sensor and Bluetooth. If the attacker is sitting in the car, he can attack from the following attack surfaces including In-Vehicle Infotainment, USB, OBD-II. In Fig 3, although OBD and USB appear to be short-range attack surfaces, they can be combined with remote attack surfaces to attack [24]. We don’t consider Denial of Service (DoS) attacks.

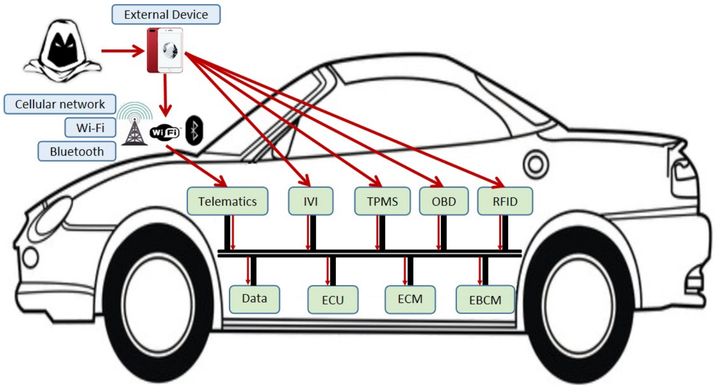

Fig 3. FFS identification scheme.

https://doi.org/10.1371/journal.pone.0239043.g003

Security threat assessment

When attackers implement the proposed attack model, the vehicle will face numerous threats as follows.

Eavesdropping attack: it mainly steals user privacy, communication units and data frames on the vehicle network, resulting in privacy information leakage.

Replay attack: The damaged external device repeatedly sends valid data to the communication units, which may affect the normal operation of the communication units. Data frames on the CAN network are repeatedly acquired and broadcast to the CAN network, which affects the normal operation of other ECUs.

Forgery attack: forge a legitimate external device or communication unit and broadcast malicious data frames to the CAN network to affect the normal operation of other ECUs.

Tampering attack: The data information between the external device and the communication units has been tampered with. tampering with eavesdropped data frames and broadcasting them to the CAN network, thereby deceiving the ECU.

If an illegal external device successfully deceives the in-vehicle communication unit, it will pose a huge threat to the vehicle and even threaten the safety of passengers' property and life. This is because external devices will attack the vehicle network through various vulnerabilities in the vehicle, such as broadcasting malicious data frames to the CAN network, and then ECUs will execute this fake instruction. Moreover, once the in-vehicle communication units are attacked, not only the vehicle networks will collapse, but also the vehicle ad hoc networks will be destroyed, which will also affect other vehicles or other legitimate external devices accordingly. According to the above attack model and evaluation results, security measures such as identity authentication of external devices and encryption of communication data should be adopted, so that combined with in-vehicle security protocols can effectively resist these threats.

The proposed scheme

Zero-knowledge proof is that the prover can make the verifier believe that a certain conclusion is correct without providing the verifier with any useful information, which has better security. We adopted this method to hide the private key information of the prover. Furthermore, we chose the FFS zero-knowledge identity authentication based on QR, because the calculation amount of its one-round authentication is not particularly large, and it can be applied to ECUs whose computing power is not particularly high. However, the FFS scheme requires many rounds of certification, which limits its application to a certain extent, such as a high-velocity connected car environment. If the FFS scheme can be further optimized and improved, it would be better.

In order to better describe our protocols, the main notations in the scheme are summarized in the Table 1. As shown in Fig 4, the designed effective and safe identity authentication scheme mainly includes the following two parts:

System initialization: the Trusted Authority (TA) first initializes the system to calculate and disclose system parameters, and then distributes public-private key pairs and calculates identity authentication parameters for the mobile phone and vehicle-mounted terminals applying for registration.

Identity authentication: The proposed scheme is adopted between the mobile phone and the vehicle, which avoids sending certificates to trusted authorities, improves the efficiency of node identity authentication, and addresses privacy issues in the process.

System initialization

As shown in Fig 5, after the ED sends the registration request, TA selects two large prime numbers p and q, calculates $n = p^* q$, and make the parameter n public. TA selects $k(k \geq 2)$ random integers that are prime and different from each other as the private keys $s_1, s_2, \ldots, s_k (1 \leq s_i <, 1 \leq i \leq k)$, calculates the corresponding public keys $v_1, v_2, \ldots, v_k (v_i = s_i^{-2} \bmod n)$, and then signs the public keys to generate $\delta_{EDv} = E_{SK_{TA}}(v_1 \| v_2 \| \ldots \| v_k \| ID_{ED} \| ID_{TA} \| TS)$. Finally, these parameters are secretly sent to the registered external device. It is assumed that the registered external device and the vehicle have downloaded or saved the public key PK_{TA} of TA. It is assumed that the vehicle has already been registered. Here we only considered the detailed initialization of ED.

Identity authentication

For a better description, the external device is referred to as ED, and the vehicle is referred to as CU (i.e., communication unit). After the system initialization, we proposed two schemes for CU to ED authentication. As shown in Algorithm 1 and Fig 6, the basic scheme is that CU authenticates the identity of ED for the first time. Concrete steps are as follows.

Table 1. Notations used for protocol.

Notation	Description
PK_{TA}	Public key of TA
SK_{TA}	Private key of TA
$H()$	Hash function
$HMAC()$	Hash function value
δ_{EDv}	Signature
CTR_x	Message counter value of x
$E()$	Encryption function
s	The prover's private key
v	The prover's public key
TS	Time stamp
ID_i	Identity of i
l_x	Time to generate x in algorithm
l_y	Time to generate y in algorithm
l_h	Time to generate hash value

https://doi.org/10.1371/journal.pone.0239043.t001

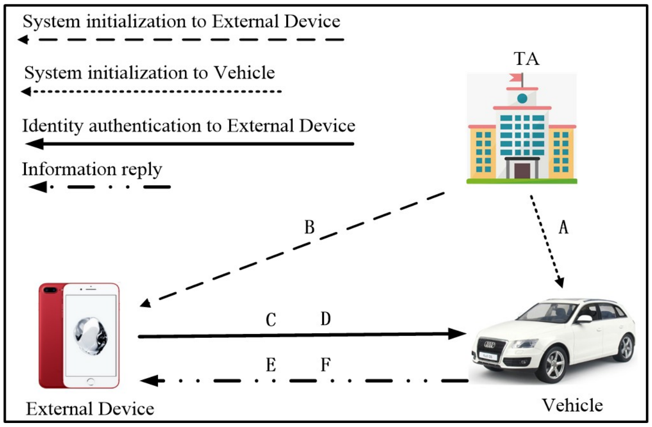
System initialization to External Device
System initialization to Vehicle
Identity authentication to External Device
Information reply
TA
A
B
C
D
E
F
External Device
Vehicle

Fig 4. System model. A represents for the message sent by TA to Vehicle, including TA's public key PK_{TA} and parameters. B represents for the message sent by TA to ED, including signature δ_{EDv}, ED's public key v_i and private key s_i. C-F represents the messages passed in the process of identity authentication. The order of A-F is defined according to the order of events.

https://doi.org/10.1371/journal.pone.0239043.g004

Step 1: ED chooses random number r, where $r<n$, and compute x by (6) and $HMCA(\cdot)_1$ by (7), Then, ED sends $Msg_1(x||\delta_{EDv}||HMCA(\cdot)_1)$ to CU. ED increases CTR_{ED} by 1.

$$x \equiv r^2 \bmod n \tag{6}$$

$$HMCA(\cdot)_1 = H(CTR_{ED}||x||ID_{ED}) \tag{7}$$

Step 2: After receiving message Msg_1, CU uses the hash function $H()$ to generate $HMCA(\cdot)_1^*$ for CTR_{ED}, x, and ID_{ED} by (8), and compares it with $HMCA(\cdot)_1$ in Msg_1 to ensure the validity of Msg_1. After successful verification, CU decrypts δ_{EDv} in Msg_1 by PK_{TA} and check $ID_{ED}||ID_{TA}||TS$. If $ID_{ED}||ID_{TA}||TS$ are valid, CU saves ID_{ED} and $v_1||v_2||...v_k$ to the secure storage. Further, CU randomly selects k-bit binary bit strings $b_1||b_2||...b_k$ and compute $HMCA(\cdot)_2$ by (9). Finally, CU sends $Msg_2(B||HMCA(\cdot)_2||)$ to ED, where B is $b_1||b_2||...b_k$. CU increases CTR_{ED} and CTR_{CU} by 1.

$$HMAC(\cdot)_1^* = H(CTR_{ED}||x||ID_{ED}) \tag{8}$$

$$HMAC(\cdot)_2 = H(CTR_{CU}||B||ID_{CU}) \tag{9}$$

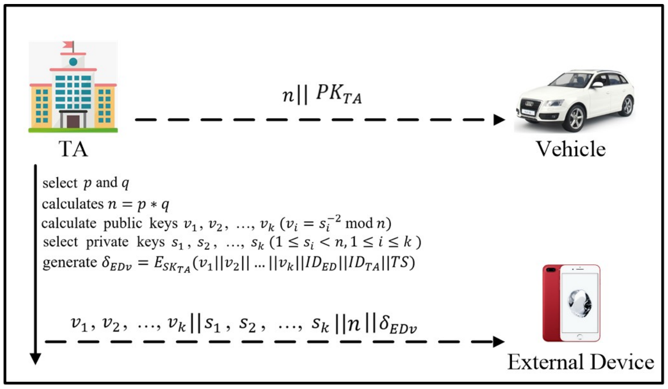
$n||\ PK_{TA}$
TA
Vehicle
select p and q
calculates $n = p * q$
calculate public keys $v_1, v_2, \ldots, v_k$ ($v_i = s_i^{-2} \bmod n$)
select private keys $s_1, s_2, \ldots, s_k$ ($1 \le s_i < n, 1 \le i \le k$)
generate $\delta_{EDv} = E_{SK_{TA}}(v_1||v_2||\ldots||v_k||ID_{ED}||ID_{TA}||TS)$
$v_1, v_2, \ldots, v_k||s_1, s_2, \ldots, s_k||n||\delta_{EDv}$
External Device

Fig 5. System initialization.

https://doi.org/10.1371/journal.pone.0239043.g005

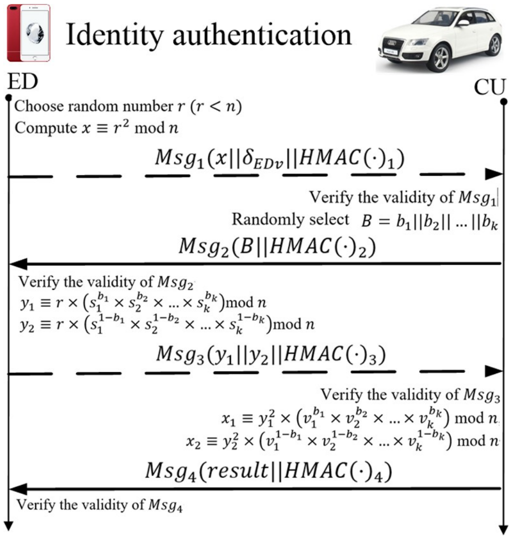
Identity authentication
ED
CU
Choose random number r ($r < n$)
Compute $x \equiv r^2$ mod n
$Msg_1(x||\delta_{EDv}||HMAC(\cdot)_1)$
Verify the validity of Msg_1
Randomly select $B = b_1||b_2|| \ldots ||b_k$
$Msg_2(B||HMAC(\cdot)_2)$
Verify the validity of Msg_2
$y_1 \equiv r \times (s_1^{b_1} \times s_2^{b_2} \times \ldots \times s_k^{b_k})\text{mod } n$
$y_2 \equiv r \times (s_1^{1-b_1} \times s_2^{1-b_2} \times \ldots \times s_k^{1-b_k})\text{mod } n$
$Msg_3(y_1||y_2||HMAC(\cdot)_3)$
Verify the validity of Msg_3
$x_1 \equiv y_1^2 \times (v_1^{b_1} \times v_2^{b_2} \times \ldots \times v_k^{b_k})$ mod n
$x_2 \equiv y_2^2 \times (v_1^{1-b_1} \times v_2^{1-b_2} \times \ldots \times v_k^{1-b_k})$ mod n
$Msg_4(result||HMAC(\cdot)_4)$
Verify the validity of Msg_4

Fig 6. Identity authentication.

https://doi.org/10.1371/journal.pone.0239043.g006

Step 3: After receiving message Msg_2, ED uses the hash function $H()$ to generate $HMCA(\cdot)_2^*$ for CTR_{CU}, B, and ID_{CU} by (10), and compares it with $HMCA(\cdot)_2$ in Msg_2 to ensure the validity of Msg_2. After successful verification, ED computes y_1 by (11), y_2 by (12) and $HMCA(\cdot)_3$ by (13). Finally, ED sends $Msg_3(y_1||y_2||HMCA(\cdot)_3)$ to CU. ED increases CTR_{ED} and CTR_{CU} by 1.

$$HMAC(\cdot)_2^* = H(CTR_{CU}||B||ID_{CU}) \tag{10}$$

$$y_1 \equiv r \times (s_1^{b_1} \times s_2^{b_2} \times \ldots \times s_k^{b_k})\text{mod } n \tag{11}$$

$$y_2 \equiv r \times (s_1^{1-b_1} \times s_2^{1-b_2} \times \ldots \times s_k^{1-b_k})\text{mod } n \tag{12}$$

$$HMAC(\cdot)_3 = H(CTR_{ED}||y_1|||y_2||ID_{ED}) \tag{13}$$

Step 4: After receiving message Msg_3, CU uses the hash function $H()$ to generate $HMCA(\cdot)_3^*$ for CTR_{ED}, y_1, y_2 and ID_{ED} by (14), and compares it with $HMCA(\cdot)_3$ in Msg_3 to ensure the validity of Msg_3. After successful verification, CU compute x_1 and x_2 by (15) and (16). If $x = x_1 = x_2$, ED is successfully authenticated by CU and CU sends $Msg_4(result||HMCA(\cdot)_4)$ to ED, where $result$ is 1 and $HMCA(\cdot)_4$ is computed by (17). Otherwise, ED is not authenticated by CU and CU sends $Msg_4(result||HMCA(\cdot)_4)$ to ED, where $result$ is 0 and $HMCA(\cdot)_4$ is computed by (12). CU increases CTR_{ED} and CTR_{CU} by 1.

$$HMAC(\cdot)_3^* = H(CTR_{ED}||y_1||y_2||ID_{ED}) \tag{14}$$

$$x_1 \equiv y_1^2 \times (v_1^{b_1} \times v_1^{b_2} \times \ldots \times v_k^{b_k)})\text{mod } n \tag{15}$$

$$x_2 \equiv y_2^2 \times (v_1^{1-b_1} \times v_1^{1-b_2} \times \ldots \times v_k^{1-b_k})\text{mod } n \tag{16}$$

$$HMAC(\cdot)_4 = H(CTR_{CU}||result||ID_{CU}) \tag{17}$$

Step 5: After receiving message Msg_4, ED uses the hash function $H()$ to generate $HMCA(\cdot)_4^*$

for CTR_{ED}, y_1,y_2 and ID_{ED} by (18), and compares it with $HMCA(\cdot)_4$ in Msg_4 to ensure the validity of Msg_4. After successful verification, if *result* is 1, ED is successfully authenticated by CU. Otherwise, ED is not authenticated by CU. ED increases CTR_{CU} by 1.

$$HMAC(\cdot)_4^* = H(CTR_{CU}||result||ID_{CU}) \tag{18}$$

Algorithm 1 Authentication Protocol

```
1: ED: Choose random number $r(r<n)$
     Compute $x = r^2 \bmod n$
   ED→CU:$Msg_1(x\|\delta_{EDv}\|HMCA(\cdot)_1)$
     Where $HMCA(\cdot)_1 = H(CTR_{ED}\|x\|ID_{ED})$
   $CTR_{ED}$++
2: CU: Verify the validity of $Msg_1$
   If $HMCA(\cdot)_1$ are valid then
     Decrypt $\delta_{EDv}$ in $Msg_1$ by $PK_{TA}$ and check $ID_{ED}\|ID_{TA}\|TS$
     If $ID_{ED}\|ID_{TA}\|TS$ are valid, then Obtain $v_1\|v_2\|\ldots v_k$
       Randomly select k-bit binary bit strings $b_1\|b_2\|\ldots b_k$
       CU→ED: $Msg_2(B\|HMCA(\cdot)_2\|)$
         Where $B = b_1\|b_2\|\ldots b_k$,
           $HMCA(\cdot)_2 = H(CTR_{CU}\|B\|ID_{CU})$
       $CTR_{CU}$++, $CTR_{ED}$++
     else Refuse the request information
   else Refuse the request information
   endif
3: ED: Verify the validity of $Msg_2$
   if $HMCA(\cdot)_2$ are valid then Compute

        $y_1 \equiv r \times (s_1^{b_1} \times s_2^{b_2} \times \ldots \times s_k^{b_k}) \bmod n$

        $y_2 \equiv r \times (s_1^{1-b_1} \times s_2^{1-b_2} \times \ldots \times s_k^{1-b_k}) \bmod n$

     ED→CU:$Msg_3(y_1\|y_2\|HMCA(\cdot)_3\|)$
       Where $HMCA(\cdot)_2 = H(CTR_{ED}\|y_1\|y_2\|ID_{ED})$
     $CTR_{CU}$ ++, $CTR_{ED}$++
   else Refuse the information
   endif
4: CU: Verify the validity of $Msg_3$
   if $HMCA(\cdot)_3$ are valid then Compute

        $x_1 \equiv y_1^2 \times (v_1^{b_1} \times v_2^{b_2} \times \ldots \times v_k^{b_k}) \bmod n,$

        $x_2 \equiv y_2^2 \times (v_1^{1-b_1} \times v_2^{1-b_2} \times \ldots \times v_k^{1-b_k}) \bmod n$

     if $x = x_1 = x_2$ then
       CU→ED: $Msg_4(result\|HMCA(\cdot)_4\|)$
         Where $result$ = 1 and $HMCA(\cdot)_4 = H(CTR_{CU}\|result\|ID_{CU})$
     else CU→ED: $Msg_4(result\|HMCA(\cdot)_4\|)$
         Where $result$ = 0 and $HMCA(\cdot)_4 = H(CTR_{CU}\|result\|ID_{CU})$
       $CTR_{CU}$ ++, $CTR_{ED}$++
   else Refuse the information
   endif
5: ED: Verify the validity of $Msg_4$
    if $HMCA(\cdot)_4$ are valid and $result$ = 1
     then ED is successfully authenticated by CU
   else ED is not authenticated by CU.
   $CTR_{CU}$ ++
endif
```

The enhanced scheme is based on the basic scheme. When the CU authenticates the ED for the first time, the information such as the ID of the ED and the public key $v_1 \| v_2 \| \ldots v_k$ has been stored by CU. In future identity authentication, it is not necessary to send the signature δ_{EDv} in Algorithm 1, and Other processes remain unchanged. It is worth noting that the calculation overhead of the enhanced scheme is less than the calculation overhead of the basic scheme, which saves authentication time.

Security analysis of the proposed protocol

In order to verify the security of this scheme, in this section, we present the following theoretical proof.

Theorem 1. If the QR problem is difficult and the assumption is true, the proposed protocol can guarantee the security of the private key s and prevent the leakage of information (i.e., the probability that the attacker A calculates a valid private key from the public key is exceedingly negligible).

Proof 1. It is assumed that A can construct the algorithm F_{QR} to solve the QR difficulty problem. The advantage of A's successful attack on x is defined as Adv_A^x.

F_{QR} publishes the public parameter $\{n, v, H\}$ and saves the public-private key pairs: $s_F \in Z_n^*$, $v_F = s_F^{-2} \bmod n$. A can query F_{QR} for q_{QR} times at most.

Query: A makes queries on random number and key. Then, F_{QR} returns $x = r^2 \bmod n$ and $v = s^{-2} \bmod n$ to A.

Challenge: A uses F_{QR} to get $r = F_{QR}(x, n)$ and $s = F_{QR}(v, n)$, respectively. That is given x and n, and r is obtained by computing.

The advantages of four successful challenges in this process are $Adv_A^r = q_{QR} * Adv_{QR}^r$ and $Adv_A^s = q_{QR} * Adv_{QR}^s$, respectively. According to the difficult problem mentioned above, the advantage Adv_A^x of the algorithm F_{QR} successfully solving the QR difficulty problem in the polynomial time is negligible. Therefore, the attacker A cannot obtain random number r and key s in $x = r^2\ modn$ and $v = s^{-2}\ modn$.

Theorem 2. Our protocol can guarantee the confidentiality and integrity of the message m, which can prevent information tampering attack, information disclosure and forgery attack.

Proof 2. Our protocol uses hash function $H(m)$ to realize the confidentiality and integrity of the message m. In order to prevent the attacker from forging legal data frames, we add the counter CTR_x and identity ID_x to the $H()$ function.

Theorem 3. Our scheme meets completeness, which meaning that honest verifier always accepts proof from honest prover.

Proof 3. Since our scheme is based on FFS, it also has completeness property.

Theorem 4. Our scheme meets soundness, which means that honest verifier never accepts proof from cheating prover since it is computationally more secure than the original FFS. In other words, as long as the number of bits of large composite number n meets the required security requirements, our scheme can almost resist guessing attacks.

Proof 4. If the attacker wants to forge a legitimate identity with public key $v_i^{b_i'}$ to cheat the verifier, he needs to compute responses y_1 and y_2. Suppose the attacker has computed x in (14), and b_i' are equal to b_i. Naturally y_1 is equal to r in (20). Next, compute y_2, which means that compute X in (21). Then, x and y_2 are substituted into Eq (16) to compute X in (22). It can be seen that because of $b_i \epsilon \{0,1\}$, the result of X is multiplied by these private keys s_i or their inverses s_i^{-1}. The QR difficulty problem has been mentioned in the previous section. It is obvious here that the attacker cannot compute y_2, which means that the probability of successful impersonation of the best attack depends on the difficulty of factoring n rather than 2^{-kt}.

$$x \equiv r^2 \times (v_1^{b_1'} \times v_2^{b_2'} \times \ldots \times v_k^{b_k'}) \bmod n \tag{19}$$

$$y_1 \equiv r \bmod n \tag{20}$$

$$y_2 \equiv r \times X \bmod n \tag{21}$$

$$\begin{aligned} X &\equiv \sqrt{\frac{v_1^{b_1'} \times v_2^{b_2'} \times \ldots \times v_k^{b_k'}}{v_1^{1-b_1} \times v_2^{1-b_2} \times \ldots \times v_k^{1-b_k}}} \bmod n \\ &\equiv \sqrt{\frac{s_1^{-b_1} \times s_2^{-b_2} \times \ldots \times s_k^{-b_k}}{v_1^{1-b_1} \times v_2^{1-b_2} \times \ldots \times v_k^{1-b_k}}} \bmod n \\ &\equiv \prod_{i=1}^{k} s_i^{1-2b_i} \bmod n \end{aligned} \tag{22}$$

Theorem 5. Our scheme meets zero-knowledge, which meaning that cheating verifier is never able to learn the prover's secret.

Proof 5. The method of proof is to construct a simulator *Sim* with the same computing resources as Verifier (V), which is indistinguishable from the real authentication process in polynomial time. *Sim* is used to generate legal interactive content.

Query 1: *Sim* makes queries, randomly chooses x, and sends x to V. Then, Verifier returns $B = b_1||b_2||\ldots||b_k$ to *Sim*.

Challenge 1: *Sim* randomly chooses r, computes $x \equiv \frac{r^2}{v_1^{b_1} \times v_2^{b_2} \times \ldots \times v_k^{b_k}} \bmod n$.

Query 2: *Sim* interacts with V again and sends x of Challenge 1 to V. Then, V returns $B = b_1||b_2||\ldots||b_k$ to *Sim*.

Challenge 2: *Sim* sends r of Challenge 1 to V.

Obviously, the output y_1' and y_2' of *Sim* and the output y_1 and y_2 of V are the same distribution, which are indistinguishable in polynomial time. When $B = 0$ and $k > 1$, V will get $z = s_1 \times s_2 \times s_k \bmod n$. According to the difficult problem mentioned above and Proof 1, the advantage

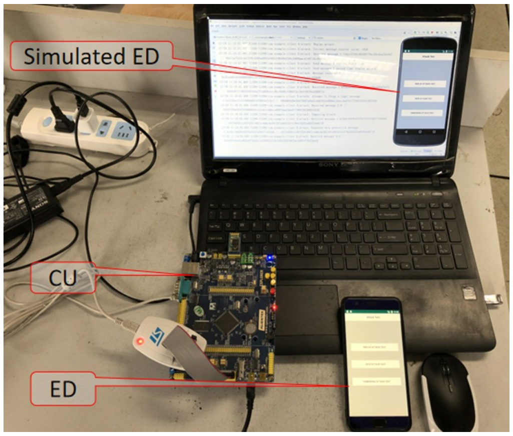

Fig 7. Hardware experimental environment.

https://doi.org/10.1371/journal.pone.0239043.g007

Table 2. Notations used for protocol.

Tools	Remarks
CU	STM32, 400MHz
Complier	Keil uVision5 (MDK5)
Software	JavaEE(SpringMVC)
PC	Used to install these software packages
ED	Android mobile phone
Bluetooth	Bluetooth 2.0
TA	Bmob cloud

https://doi.org/10.1371/journal.pone.0239043.t002

$Adv^{s}_{Verifier}$ of the algorithm F_{DL} successfully solving the QR difficulty problem in the polynomial time is negligible. Obviously, apart from convincing *Sim*, V cannot get any valuable information. Therefore, the scheme has zero-knowledge property under parallel composition.

Simulation evaluation

In this section, to evaluate the performance and security of the protocols, we constructed a hardware experimental environment, which can be found in Fig 7. This experiment used STMicroelectronics' automotive microcontrollers, which is a high-performance 32-bit ARM Cortex®-M7 MCU developed by ST. The maximum operating frequency is 400MHz. We used a CU with a Bluetooth serial port and connected the CU to the ED via a Bluetooth module. The specifications of the tools employed in the hardware and software in the experiment are shown in Table 2. Firstly, we ported Contiki to Keil's MDK5 integration environment to compile the code used in the experiment and import the code into processors using ST-LINK V2. Secondly, we used Android to develop a simulated mobile phone on the computer as an ED and developed a corresponding Application (APP) for the proposed scheme to facilitate the implementation of the authentication. The simulated mobile phone system can be implanted on Android phones. Finally, we create Bmob cloud users based on JavaEE (SpringMVC) as a third-party trusted TA. In addition, we use JavaEE(SpringMVC) to develop a server-side to observe identity authentication process of the simulated CU and ED.

In order to make our protocol more advantageous, we compared the average time delays of authentication at different clock rates (400, 300, 200, 168, 150, and 120 MHz) with the average time delays of NOTSA's authentication [23] and POSTER's authentication [36]. Compared with

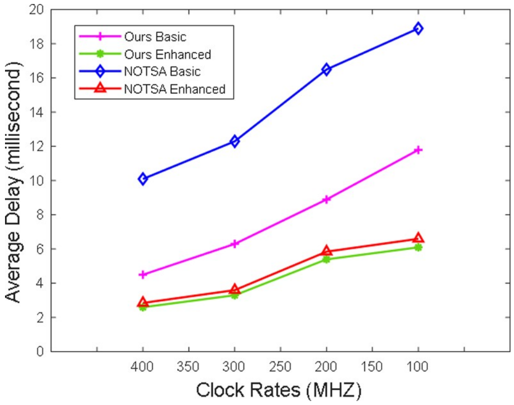

Fig 8. Comparison among ours and NOTSA at different clock rates.

https://doi.org/10.1371/journal.pone.0239043.g008

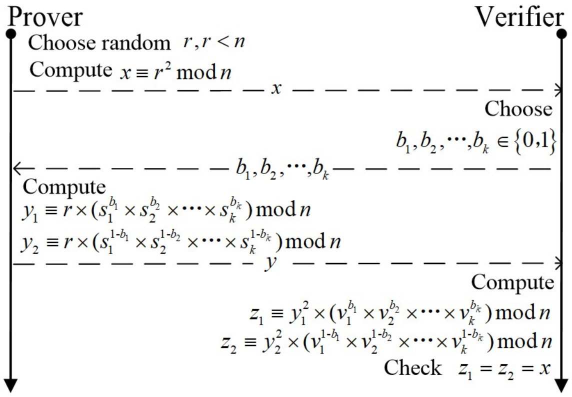
Prover
Verifier
Choose random $r, r < n$
Compute $x \equiv r^2 \bmod n$
x
Choose
$b_1, b_2, \cdots, b_k \in \{0,1\}$
$b_1, b_2, \cdots, b_k$
Compute
$y_1 \equiv r \times (s_1^{b_1} \times s_2^{b_2} \times \cdots \times s_k^{b_k}) \bmod n$
$y_2 \equiv r \times (s_1^{1-b_1} \times s_2^{1-b_2} \times \cdots \times s_k^{1-b_k}) \bmod n$
y
Compute
$z_1 \equiv y_1^2 \times (v_1^{b_1} \times v_2^{b_2} \times \cdots \times v_k^{b_k}) \bmod n$
$z_2 \equiv y_2^2 \times (v_1^{1-b_1} \times v_2^{1-b_2} \times \cdots \times v_k^{1-b_k}) \bmod n$
Check $z_1 = z_2 = x$

Fig 9. The proposed scheme with removing the hash function, counter value, etc.

https://doi.org/10.1371/journal.pone.0239043.g009

NOTSA, the proposed scheme has a smaller calculation amount, so the average time delays of ours are shorter, as shown in Fig 8. At different clock rates, the average time delays of our enhanced scheme are under 6.1 ms at different clock rates. In addition, average time delays of POSTER's the zero-knowledge proofs of are between 75–217 ms, which is much more than ours.

Simplify our scheme into the form of FFS scheme (e.g., remove the hash function, counter value, etc.), as shown in Fig 9. Then, the simplified scheme is compared with FFS and DFFS [33]. In order to make experimental data conveniently, we did simulation experiments on PC and compare the average delay of each scheme at different values of k and t, as shown in Fig 10. In the FFS scheme, the probability of soundness is 2-kt, which is obviously based on the size values of the k and t parameters. When the value of t is larger, the more times the prover interacts with the verifier, the longer the authentication delay. When the value of k is larger, the number of public and private keys stored is larger, and the harder it is to save and process. From the above section, it is worth mentioning that our scheme can achieve extremely high soundness with only one iteration of authentication, which is based on the QR difficult problem. In the DFFS scheme, it is an improved 3-pass parallel interactive scheme with 'almost' zero soundness error, which is based on FFS digital signature. The probability of soundness error (or cheating probability) is $2^{-(kt+h/2)}$. The DFFS scheme requires encryption and decryption of hash and the promised x value for each iteration of authentication. When the value of k is too large, especially when it is greater than 100, its authentication time delays will increase

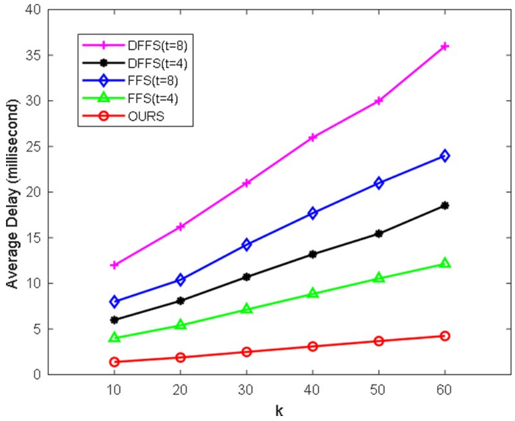

Fig 10. Comparison among DFFS, FFS, and ours at different values of k and t.

https://doi.org/10.1371/journal.pone.0239043.g010

Table 3. Computational costs comparison.

Scheme	FFS	DFFS	OURS
n (bit)	1024	1024	1024
The number of keys *s*	k	k	k
Number of authentication rounds	t	t	1
Is there a hash function?	No	SHA1	No
Communication overhead	$t(2048 + k)$	$t(2048 + k)$	$3072 + k$
Computational overhead	$t(l_x + 2l_y)$	$t(l_x + 4l_y + 2l_h)$	$l_x + 4l_y$

https://doi.org/10.1371/journal.pone.0239043.t003

exponentially. Although the cheating probability is reduced, the computational overhead is increased, and the number of authentication iterations is still t. In our scheme, the idea of "two-to-one" (e.g., y_1 and y_2 correspond to x) and "reversal" (e.g., b and $1-b$) can make it possible to have extremely high security in one iteration of authentication. In order to make the comparison schemes more impressive, a computational costs comparison table is given, as shown in Table 3. Therefore, our proposed scheme has higher security and efficiency, and it can meet extremely high soundness in one iteration of authentication.

Conclusions

In this paper, we present the main attack models and security threat assessments for vehicles. Then, on this basis, we designed an efficient and safe identity authentication scheme based on Feige-Fiat-Shamir identification scheme with extremely high soundness. The proposed scheme has extremely high soundness based on the quadratic residue (QR) difficult problem. Subsequently, we analyzed the security of the proposed solution through a safety certificate. In simulation and evaluation, we built a hardware lab environment to evaluate performance. At the same time, software simulation was performed using JavaEE (SpringMVC) and Android. The experimental results prove that the proposed scheme is feasible and highly effective. In the future, the number of nodes in the Internet of Vehicles will increase rapidly. If each identity authentication is interactive, there may be some delays, which does not meet the high speed requirements of the Internet of Vehicles. Therefore, we will further study non-interactive zero-knowledge proofs for more secure and efficient authentication.

Supporting information

S1 File.
(RAR)

S2 File.
(RAR)

S3 File.
(JAVA)

S4 File.
(JAVA)

Acknowledgments

We would like to thank the Editor and the reviewers for their constructive comments and helpful suggestions.

Author Contributions

Conceptualization: Mu Han, Zhikun Yin.

Data curation: Mu Han.

Formal analysis: Mu Han, Zhikun Yin.

Funding acquisition: Mu Han, Xing Zhang, Shidian Ma.

Investigation: Mu Han, Zhikun Yin.

Methodology: Mu Han, Zhikun Yin.

Project administration: Mu Han.

Resources: Mu Han.

Software: Pengzhou Cheng.

Supervision: Mu Han, Xing Zhang, Shidian Ma.

Validation: Mu Han.

Visualization: Mu Han.

Writing – original draft: Zhikun Yin.

Writing – review & editing: Mu Han.

References

1. Yang D, Jiang K, Zhao D, Yu C, Cao Z, Xie S, et al. Intelligent and connected vehicles: Current status and future perspectives. Sci China. Tec Sci., 2018, 61, 1446–1471. https://doi.org/10.1007/s11431-017-9338-1
2. Ring T. Connected cars–the next target for hackers. Net. Secu., 2015, 2015, 11–16.
3. Wu W. et al., "A Survey of Intrusion Detection for In-Vehicle Networks," in IEEE Trans. on Intell. Trans. Sys., vol. 21, no. 3, pp. 919–933, March 2020. https://doi.org/10.1109/TITS.2019.2908074
4. Othmane L B, Weffers H, Mohamad M M, Wolf M. A survey of security and privacy in connected vehicles. Proc. Wire. Sen. Mob. Ad. Net., Springer, 2015, 217–247.
5. Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle. Proc. Black Hat, Las Vegas, NV, USA, 2015, 1–91.
6. Nie S, Liu L, Du Y. Free-fall: Hacking tesla from wireless to can bus. Briefing, Black Hat USA, 2017, 2017,1–16.
7. Tencent Keen Security Lab. Oct. 28, 2019. Experimental Security Research of Tesla Autopilot. https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf
8. Xiangxue L, Yu Y, Guannan S. Connected Vehicles' Security from the Perspective of the In-Vehicle Network. IEEE Net., 2018, 32, 58–63.
9. Cho K T, Shin K G. Viden: Attacker identification on in-vehicle networks. Proc. ACM SIGSAC Conf. Com. Commun. Sec., ACM, 2017, 1109–1123.
10. Mundhenk P, Paverd A, Mrowca A, Steinhorst S, Lukasiewycz M, Fahmy S A, et al. Security in automotive networks: Lightweight authentication and authorization, ACM Trans. Des. Auto. Elect. Syst., 2017, 22, 1–27. https://doi.org/10.1145/2960407
11. Ansari M R, Yu S C, Yu Q Y. IntelliCAN: Attack-resilient controller area network (CAN) for secure automobiles. Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst., 2015, 233–236.
12. Kim J H. Gateway framework for in-vehicle networks based on can, flflexray, and Ethernet. IEEE Trans. Veh. Technol., 2015, 64, 4472–4486.
13. Woo S, Jo H J, Kim I S, Lee D H. A practical security architecture for in-vehicle CAN-FD. IEEE Trans. Intell. Transp. Syst., 2016, 17, 2248–2261.
14. Bagga P, Das A K, Wazid M, Rodrigues J J P C and Park Y, "Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges," in IEEE Access, vol. 8, pp. 54314–54344, 2020

15. Groza B, Murvay S. Effiicient protocols for secure broadcast in controller area networks. IEEE Trans. Ind. Informat., 2013, 9, 2034–2042.

16. Shamir A. Identity-based cryptosystems and signature schemes, Workshop on the Theory and Application of Cryptographic Techniques, Springer, Berlin, Heidelberg, 1984. 47–53.

17. Feige U, Fiat A, Shamir A. Zero-knowledge proofs of Identity, Journal of Cryptology, 1988, 1, 77–94.

18. Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. proceeding of CRYPTO '86, Lecture Notes in Computer Science, Springer-Verlang, Berlin, 1987, 263, 186–194.

19. Kumari S, Chaudhry S A, Wu F et al. An improved smart card based authentication scheme for session initiation protocol. Peer-to-Peer Netw. 2017, 10, 92–105. https://doi.org/10.1371/journal.pone.0213688

20. Chim T W, Yiu S M, Hui L C K, Li V O K. SPECS: Secure and privacy enhancing communications schemes for VANETs. Ad. Hoc. Netw. 2011, 9, 189–203.

21. Horng S J, Tzeng S F, Pan Y, Fan P, Wang X, Li T, et al. b-SPECS+: Batch verification for secure pseudonymous authentication in VANET. IEEE Trans. Inf. Forens. Secur. 2013, 8, 1860–1875.

22. Tsai J L, Lo N W. A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Syst. J.,2015, 9, 805–815. https://doi.org/10.1109/JSYST.2016.2574719

23. Wang L, Liu X. NOTSA: Novel OBU with Three-level Security Architecture for Internet of Vehicles, IEEE Internet of Things Journal, 2018, 5, 3548–3558.

24. Woo S, Jo H J, Lee D H. A practical wireless attack on the connected car and security protocol for in-vehicle can, IEEE Trans. Intell. Transp. Syst., 2015, 16, 993–1006.

25. Li X, Niu J, Kumari S, Wu F, Kim-Kwang Raymond Choo. A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city, Future Generation Computer Systems, 2018, 83, 607–618.

26. Ying B, NAYAK A. Anonymous and Lightweight Authentication for Secure Vehicular Networks. IEEE Trans. on Vehi. Tech., 2017, 66, 10626–10636.

27. Stinson D R. Cryptography Theory and Practice. CRC Press, 1995.

28. Mao W. Modern Cryptography: Theory and Practice. Upper Saddle River, NJ: Prentice-Hall PTR, 2003.

29. Menezes A J, van Oorschot P C, Vanstone S A. Handbook of Applied Cryptography, 1996.

30. Shoup V. On the Security of a Practical Identification Scheme, 1996,1.

31. Schneier B. Applied Cryptography, Wiley & Sons, 1994.

32. Fischer M J. CPSC 467b: Cryptography and Computer Security Lecture 18. Department of Computer Science, Yale University, 2005.

33. Dhanya RS, Megha V A. An Improved Parallel Interactive Feige-Fiat-Shamir Identification Scheme with almost zero soundness error and complete zero-knowledge. 2014 First International Conference on Networks & Soft Computing, 2014, 252–257.

34. Goldwasser S, Micali S. Probabilistic encryption. Journal of computer and system sciences, 1984, 28, 270–299.

35. Parkinson S, Ward P, Wilson K. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Transactions on Intelligent Transportation Systems, 2017, 18, 2898–2915.

36. Gabay D, Cebe M, Akkaya K. POSTER: On the Overhead of Using Zero-Knowledge Proofs for Electric Vehicle Authentication. In Proceedings of WiSec'19: ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2019, 347–348.