future internet

MDPI

Article

A V2V Identity Authentication and Key Agreement Scheme Based on Identity-Based Cryptograph

Qiang Li

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China; liqiang@bupt.edu.cn

Abstract: Cellular vehicle to everything (C-V2X) is a technology to achieve vehicle networking, which can improve traffic efficiency and traffic safety. As a special network, the C-V2X system faces many security risks. The vehicle to vehicle (V2V) communication transmits traffic condition data, driving path data, user driving habits data, and so on. It is necessary to ensure the opposite equipment is registered C-V2X equipment (installed in the vehicle), and the data transmitted between the equipment is secure. This paper proposes a V2V identity authentication and key agreement scheme based on identity-based cryptograph (IBC). The C-V2X equipment use its vehicle identification (VID) as its public key. The key management center (KMC) generates a private key for the C-V2X equipment according to its VID. The C-V2X equipment transmit secret data encrypted with the opposite equipment public key to the other equipment, they authenticate each other through a challenge response protocol based on identity-based cryptography, and they negotiate the working key used to encrypt the communication data. The scheme can secure the V2V communication with low computational cost and simple architecture and meet the lightweight and efficient communication requirements of the C-V2X system.

Keywords: C-V2X; V2V; identity authentication; key agreement; IBC

Citation: Li, Q. A V2V Identity Authentication and Key Agreement Scheme Based on Identity-Based Cryptograph. *Future Internet* **2023**, *15*, 25. https://doi.org/10.3390/fi15010025

Academic Editor: Ming-Chin Chuang

Received: 18 November 2022
Revised: 30 December 2022
Accepted: 30 December 2022
Published: 3 January 2023

1. Introduction

The Internet of Vehicles connects vehicles, roads, people, and other traffic participants through wireless networks to reduce the accident rate, improve driving safety, improve traffic efficiency, save energy, and reduce carbon emissions. The European Union, the United States, and Japan attach importance to the development of the Internet of Vehicles and have made a strategic development plan of establishing a cooperative vehicle infrastructure system. The 3GPP (3rd Generation Partnership Project), ITU (International Telecommunication Union), ETSI (European Telecommunications Standards Institute), ISO (International Organization for Standardization), and SAE (Society of Automotive Engineers) have carried out Internet of Vehicles international standard research and formulation. The U.S. Department of Transportation predicts vehicle to vehicle (V2V) communication can avoid 82% of light collisions in the United States.

There are mainly two Internet of Vehicles standards worldwide. One is C-V2X (cellular vehicle to everything, including LTE-V2X and its evolved NR-V2X); another is dedicated short range communication (DSRC, IEEE802.11p). The C-V2X is a vehicle wireless communication technology based on a cellular network which supports V2V (vehicle to vehicle), V2I (vehicle to infrastructure), V2N (vehicle to network), and other communication modes. Based on cellular mobile communication networks (4G or 5G), the C-V2X technology is innovatively designed to provide high reliability, low latency, and large bandwidth communication capabilities and support many application scenarios, such as formation driving, semi-automatic driving, extended sensor, remote driving, etc. For example, vehicles can share sensed information through V2V communication and provide reminders of road conditions, such as an accident ahead, defective vehicle, slippery road, or low visibility,

and other security events to remind other vehicles to avoid dangers. The C-V2X is the most important supporting technology to achieve an automatic driving and intelligent transportation system [1,2].

In the C-V2X system, it is necessary to authenticate the identity of the communication equipment to ensure the equipment participating in the communication are legal equipment, and it is necessary to encrypt the communication data to ensure the communication data is not stolen or forged. This paper focusing on the V2V communication scenario, proposes a lightweight equipment identity authentication and key agreement scheme.

The rest of the paper is organized as follows: Section 2 summarizes the C-V2X security risk and security technology. Section 3 analyzes the V2V identity authentication and key agreement requirement and explains the significance of this study. Section 4 introduces the identity-based cryptography technology. Section 5 proposes a lightweight V2V identity authentication and key agreement scheme. Section 6 analyzes the scheme security and builds an experimental validation environment to verify the scheme feasibility. Finally, Section 7 concludes the paper.

2. C-V2X Security Risk and Security Technology Overview

2.1. C-V2X Security Risk

With the popularization and application of C-V2X technology, the vehicle has gradually changed from a traditional transportation means to mobile equipment. Vehicle networking means it will be detected by the network anytime and anywhere and will face many network security problems. The C-V2X technology integrates communication, transportation, and automobile technologies, faces security risks, such as eavesdropping, tampering, forgery, denial of service (DoS), and so on. The C-V2X equipment integrates navigation, information entertainment, vehicle control, auxiliary driving, and other functions, which can easily become the target of hacker attacks, resulting in information leakage, an out-of-control vehicle, and other security problems. The C-V2X equipment interface is vulnerable to deception, intrusion, access control, and other attacks. The vehicle functions are designed after ISO26262 (Road Vehicles—Functional Safety), and the safety of the vehicle components has been basically validated. Thus, this paper focuses on the security of C-V2X communication.

The C-V2X system have many kinds of data with different data sources, face security risks, such as illegal access, illegal tampering, and user privacy disclosure in the process of data generation, transmission, storage, use, discarding, or destruction. The vehicle driving is related to traffic safety, personal safety, social stability, and national security. There are many pieces of equipment in the C-V2X system. The security risk in one vehicle may spread to other vehicles or even to the whole system. Therefore, whether the security problem is solved or not determines the C-V2X technology comprehensive promotion and large-scale commercial application. The security technology of the C-V2X must be developed synchronously with the C-V2X communication technology.

2.2. C-V2X Security Technology

With the gradual maturity and commercial application of C-V2X technology, its security technology has attracted more and more attention. Scholars have carried out a series of research on the C-V2X security technology, increased C-V2X security technology and standards research, formulated a perfect security scheme, and promoted the healthy development of the automobile industry and transportation industry.

The existing C-V2X security technology involves security isolation, access control, identity authentication, data encryption, data signature, data backup, and other technologies. However, overall, the C-V2X security system is still in its infancy. Scholars pay more attention to the traditional network security issues, and C-V2X personalized security technology, such as equipment efficient authentication, privacy protection, and data security-sharing technology is weak. The C-V2X security technology needs to be improved urgently.

National researchers are highly concerned about the C-V2X security technology, and there is not a unified C-V2X security standard and security scheme. Identity authentication can be used to distinguish legal equipment from malicious equipment. The C-V2X system can set different access levels for different equipment through authorization management, protect the data in the C-V2X system through data encryption, set data priority to ensure the system availability, and set an integrity check to ensure the information is not modified or deleted by malicious users [3]. The PKI (public key infrastructure) mechanism based on a public key certificate is used to ensure the security authentication and secure communication between the equipment and digital signature; encryption and other technologies are used to achieve the communication security between the equipment. The security functions, such as certificate issuance, certificate revocation, equipment information security collection, data management and exception analysis, can be achieved through the security management system. The blockchain technology is used to achieve the communication security and establish trusted relationships between the C-V2X equipment through distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm. When vehicles communicate directly through the PC5 interface, a trust relationship must be established between vehicles [4]. The general method is to authenticate the identity of the equipment based on the PKI mechanism, but in this way, the equipment needs to obtain in advance the equipment certificate from the certification authority in a secure way and requires a complex certificate verification process. Different security domains can be segmented according to geographical regions, and each domain has different security levels [5]. Data access control and encrypted data retrieval can be carried out based on roles and attributes, and vehicle data can be encrypted and protected through an access control policy and policy execution engine [6]. Privacy protection mainly includes user identity privacy protection and location privacy protection. Identity privacy is protected by group signature technology, and location privacy is protected by pseudonym change strategy and location-based service [7]. Equipment authentication and key agreement can be achieved based on the elliptic curves cryptography (ECC) algorithm to protect equipment communication security and data security [8].

3. Requirement Analysis of V2V Identity Authentication and Key Agreement

The C-V2X system security includes confidentiality (unauthorized equipment cannot obtain valid information), authentication (the sender and receiver of the information are registered equipment), and integrity (the data cannot be tampered). Cryptographic protocols need to be used to ensure the information will not be stolen, tampered, forged, and used in other attacks. The C-V2X system is complex, involves a wide variety of information, including user identity, location, route, and other privacy data. It is necessary to design appropriate security protection schemes for different scenarios.

The C-V2X equipment communicate with each other through the PC5 interface to achieve data interaction between vehicles (V2V communication). Using V2V communication, vehicles can share information, such as traffic conditions, traffic lights, and traffic flow collected by sensors with each other. The driver can enhance auxiliary driving safety with the information provided by other vehicles. Multiple vehicles cooperatively driving can achieve complex driving scenes, such as formation driving and automatic driving. The vehicles can exchange speed, position, and heading information with each other to avoid accidents, such as collisions. For example, when the vehicle in front finds a traffic accident on the road ahead, the vehicle in front will brake urgently and send the accident information to the vehicle behind. The vehicle behind will use visual, tactile, and auditory alarms to warn the driver and automatically take avoidance measures, such as braking when necessary, to avoid traffic accidents, such as rear end collisions.

The PKI mechanism based on a public key certificate is used to ensure the secure authentication and secure communication between the equipment, using digital signature and encryption. The CA (certification authority) system is a complex system and may adopt a hierarchical structure. In small- and medium-sized C-V2X systems (for example,

the Internet of Vehicles system in small- and medium-sized cities, the auto drive system in a logistics center, the vehicle management system in an industrial park, etc.), certificate verification requires large computing and time overhead and has a great impact on the communication delay. Therefore, the authentication protocol based on PKI cannot fully meet the C-V2X lightweight requirement [9]. It is not necessary for the C-V2X system to establish a complex CA system. A flat and efficient authentication and encryption scheme is needed to ensure the C-V2X system security. The V2V communication needs a low-bandwidth and low-latency security scheme [10].

4. Identity-Based Cryptograph Technology

Asymmetric cryptography uses different keys to encrypt and decrypt; the private key is saved locally, and the public key is public and can be transmitted in plaintext, solving the problem of key secure transmission in symmetric cryptography. Compared with symmetric cryptography, asymmetric cryptography has same the security, but it is easier to distribute and manage the key. In asymmetric cryptography, how to securely publish the public key and how to associate the user identity information with his key is the key problem. The PKI (public key infrastructure) system is generally used to generate, manage, store, distribute, and revoke certificates. Due to the complexity of certificate management, the PKI system is often large in the practical application with a high cost and low efficiency [11].

In the security system based on PKI, each equipment needs to apply and install a certificate to ensure communication security, which makes the equipment more complex, especially for equipment with poor computing power. The PKI system needs to establish a CA to uniformly manage the generation, issuance, storage, and revocation of the certificate; the CA is a complex system. The equipment needs to verify the opposite equipment certificate to ensure the opposite equipment is registered equipment, which requires large computing overhead. Vehicles may be running in high speed on the highway. V2V communication may transmit highly timely information, such as traffic conditions and safety accidents. The communication delay should be low, and the computational complexity should be small. The method that requires complex computation may not be suitable for many V2V communication scenarios. To reduce the complexity of key management in asymmetric cryptography system, Shamir proposed identity-based cryptography in 1984 [12,13]. The user identity can be used as the user public key, or the user public key can be calculated from the user identity by an appointment algorithm.

Identity-based cryptography is the same as traditional asymmetric cryptography. Each user has both an associated public key and a private key. In the identity-based cryptography system, the user identity, such as name, IP address, e-mail address, mobile phone number, and so on, is used as the public key, and the corresponding user private key is calculated with the public key. The user ID is the user public key, which does not need generation and storage. It only needs to publish the public key, and the private key is saved secretly by the user. The user private key is calculated by the KGC (key generation center) according to the system master key and user ID. The user public key is uniquely determined by the user ID so it does not need a third party to ensure the authenticity of the public key. The identity-based cryptography does not need key infrastructure and has better security and convenience than the PKI.

In 1999, K. Ohgishi, R. Sakai, and M. Kasahara proposed an identity-based key-sharing scheme using elliptic curve pairing. In 2001, D. Boneh, M. Franklin, R. Sakai, K. Ohgishi, and M. Kasahara proposed a method of constructing identity-based cryptography with elliptic curve pair. These works have promoted the new development of identity-based cryptography, and a number of identity-based cryptography implemented with elliptic curve pairs have emerged, including digital signature algorithm, key exchange protocol, key encapsulation mechanism, and public key encryption algorithm. For identity-based cryptograph as an asymmetric cryptography, the most prominent feature is the user does not need a certificate; the user private key is generated by the KGC based on the system master key and user identity [14]. SM9 is an identity-based cryptography standard which is

recommended by the government of China. Identity-based cryptography does not need a certificate, is simple and easy to use, and meets the high real-time application environment, such as the C-V2X system [15,16].

5. Lightweight V2V Identity Authentication and Key Agreement Scheme

Small- and medium-size C-V2X systems need a flat and efficient identity authentication and key agreement scheme to reduce the cost of construction and decrease the communication delay. Identity-based cryptograph does not require a CA system and does not need a certificate management and certificate verification process, greatly simplifying the complexity of the C-V2X system. This paper proposes a V2V identity authentication and key agreement scheme based on identity-based cryptograph which can achieve vehicle identity authentication, and the working key agreement only needs simple communication and few computing resources.

5.1. Security Architecture

The C-V2X system includes an OBU (on board unit), RSU (roadside unit), cloud platform, application, etc. To establish a security architecture, it is necessary to set up an equipment (vehicle) registration center (ERC) and a key management center (KMC) in the C-V2X system. The function of the ERC is to generate VID according to the information provided by the user. The ERC can manage the equipment information and monitor the equipment status. The KMC is the most important equipment of the C-V2X security architecture and generates the private key of the equipment according to the equipment public key (uses the equipment VID as the equipment public key) and storage, distribution, and destruction the equipment private key. The ERC and KMC provide services for the whole C-V2X system and are the core equipment of the security scheme. They are generally established in the central node of the system, such as the traffic management department. The KMC implementation based on identity-based cryptographic, has a secure storage area, random number generator, identity-based cryptographic algorithm, symmetric cryptographic algorithm, and so on. The system security architecture is shown in Figure 1.

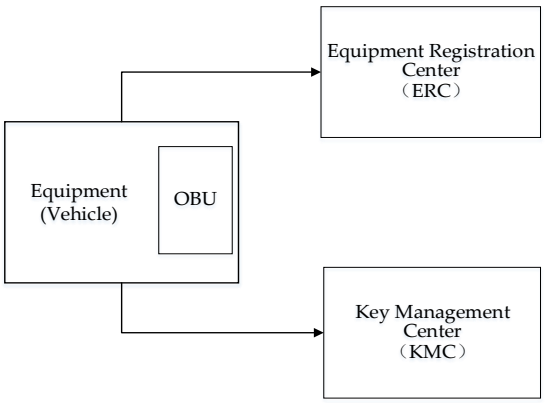

Figure 1. Security Architecture.

The ERC assigns a unique number as a VID to each C-V2X equipment with the equipment information. The VID is composed of organization code, manufacturer code, category, model, serial number, area code, and operator code [17]. The VID is the unique identification of the C-V2X equipment and is also the public key of the equipment. The private key of the equipment is generated by KMC based on the identity-based cryptographic algorithm and the public key of the equipment.

5.2. Equipment Registration and Access Process

The user reports the equipment information (include equipment manufacturer, type, model, serial number, and so on) to the ERC and registers the equipment in ERC when the equipment need access to the C-V2X system. Then, the ERC generates the equipment VID with the equipment information and saves the equipment VID and information in the internal database. The equipment saves its VID in the internal secure storage area. The equipment registration process is completed.

The equipment sends its VID to the KMC to apply for its private key when accessing the C-V2X system. The KMC uses the VID as the public key of the equipment, generates the equipment private key with the identity-based cryptographic algorithm, and sends the private key to the equipment through an internal secure channel which will be discussed in future research. The equipment saves its private key in an internal secure storage area. The equipment registration and private key generation process is shown in Figure 2.

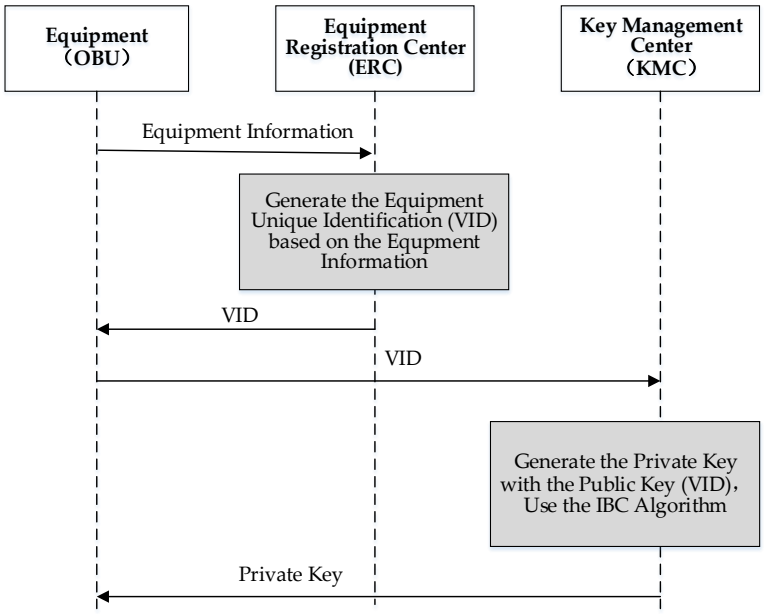

Figure 2. Equipment Registration and Private Key Generation Process.

5.3. V2V Identity Authentication and Key Agreement Process

In the C-V2X system, to ensure the communication equipment is registered equipment, identity authentication is implemented between the equipment. It is necessary to encrypt the communication data between the equipment (vehicle) to achieve data confidentiality and integrity. In the C-V2X system, the vehicle may be moving rapidly, and the process of encrypting communication data should be as fast as possible to reduce communication delay and enhance the real-time performance. Therefore, the symmetric encryption algorithm is used in V2V communication.

When Equipment (vehicle) A needs to communicate with Equipment (vehicle) B, A sends an authentication request to B. A and B authenticate each other's identities based on identity-based cryptographic technology and synchronously negotiate the subsequent encrypted working key in the authentication process. Through the authentication protocol, the equipment can confirm whether the other equipment is registered and obtain the private key from KMC. Only the equipment with a private key that matches its VID can complete the authentication process; otherwise, the authentication fails. In the authentication process, A sends a random number encrypted by the B public key to B and confirms whether B decrypted successfully by verifying the response data from B. B verifies A the same way. A and B interact with private random numbers in the authentication process. The

random numbers will be used as the material for generating the working key. The identity authentication and key agreement process is shown in Figure 3.

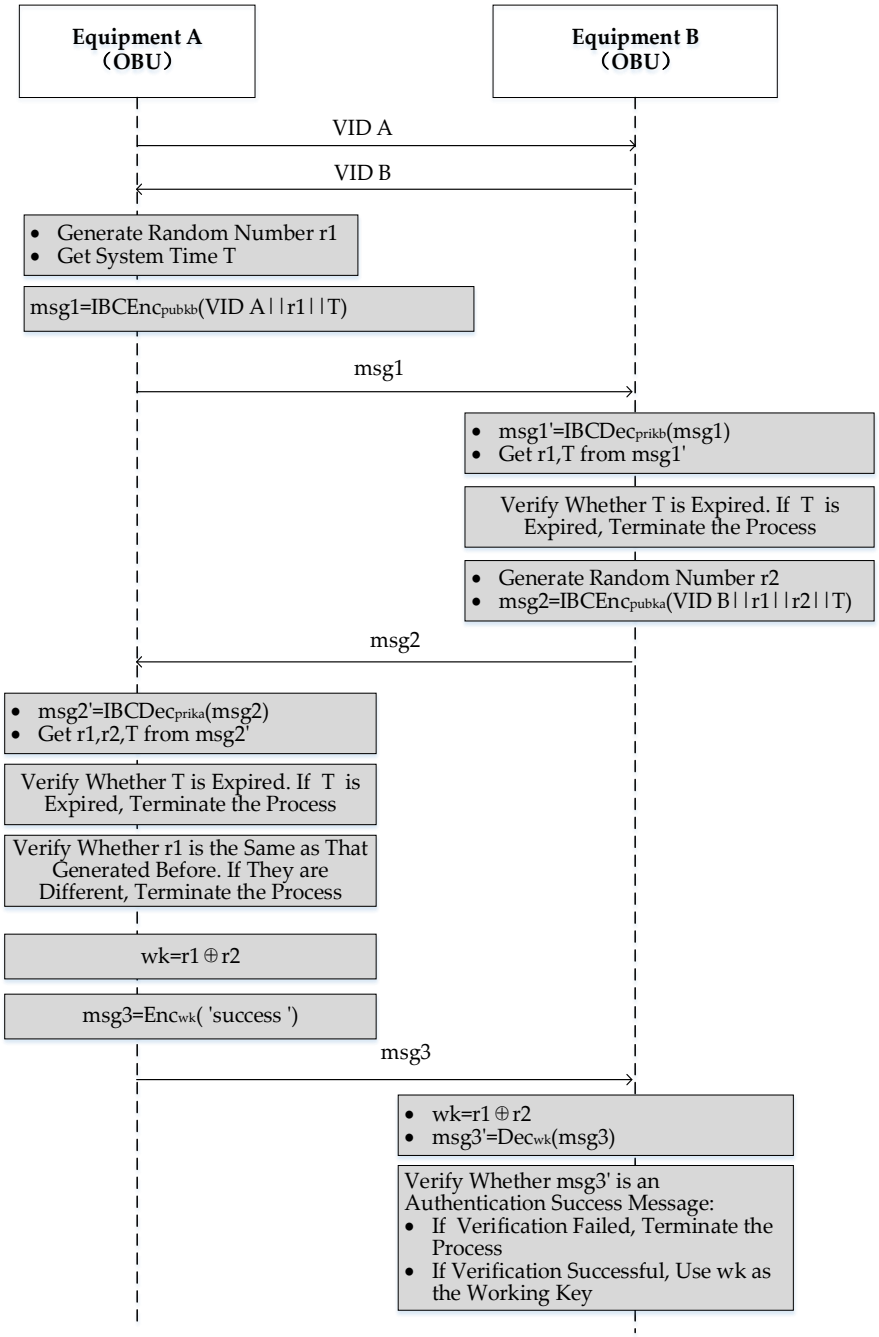

Figure 3. V2V Identity authentication and key agreement process.

(1) Equipment A sends its VID (*VID A*) to Equipment B through the PC5 interface, and *VID A* is the Equipment A public key.

(2) Equipment B sends its VID (*VID B*) to Equipment A through the PC5 interface, and *VID B* is the Equipment B public key.

(3) Equipment A generates a random number, *r1*, obtains the system time, *T*, and calculates the authentication message, *msg1*, using *VID A*, *r1*, and *T*. Equipment A sends

msg1 to Equipment B, *pubkb* is Equipment B public key (*VID B*), and *IBCEnc* represents the asymmetric encryption function. The *msg1* calculation method is as follows.

$$msg1 = IBCEnc_{pubkb}(VID\ A \| r1 \| T) \tag{1}$$

(4) Equipment B decrypts *msg1* (received from equipment A) with its private key, *prikb*, obtains *r1* and *T* from *mgs1′*; *prikb* is Equipment B's private key, and *IBCDec* represents asymmetric decryption function. Equipment B verifies whether *T* is expired. If *T* is expired, it terminates the process. The *msg1′* calculation method is as follows.

$$msg1' = IBCDec_{prikb}(msg1) \tag{2}$$

(5) Equipment B generates a random number, *r2*, calculates the authentication message *msg2* using *VID B*, *r1*, *r2*, and *T*, and sends *msg2* to Equipment A; *pubka* is Equipment A's public key. The *msg2* calculation method is as follows.

$$msg2 = IBCEnc_{pubka}(VID\ B \parallel r1 \parallel r2 \| T) \tag{3}$$

(6) Equipment A decrypts *msg2* (received from Equipment B) with its private key, *prika* and obtains *r1*, *r2*, and *T* from *msg2′*. Equipment A verifies whether *T* has expired. If *T* is expired, it terminates the process. Equipment A verifies whether *T* is the same as the *T* in *msg1* to determine whether the response is the same session. If they are different, it terminate the process.

(7) Equipment A verifies whether *r1* sent by Equipment B is *r1* generated previously. If not, it terminates the process.

(8) Here, Equipment A completes the authentication of Equipment B. Equipment A calculates the working key, *wk*, encrypts the authentication success message with working key, sends the response message, *msg3*, to Equipment B. *Enc* represents symmetric encryption function, and $\oplus$ represents XOR function. The *wk* and *msg3* calculation methods are as follows.

$$wk = r1 \oplus r2 \tag{4}$$

$$msg3 = Enc_{wk}(\text{'}success\text{'}) \tag{5}$$

(9) Equipment B calculates the working key, *wk*, and decrypts *msg3* (received from Equipment A). Dec represents the symmetric decryption function. The *wk* and *msg3′* calculation methods are as follows.

$$wk = r1 \oplus r2 \tag{6}$$

$$msg3' = Dec_{wk}(msg3) \tag{7}$$

(10) Equipment B verifies whether *msg3′* is an authentication success message. If yes, it indicates Equipment A and Equipment B use the same working key, *wk*. Here, Equipment B completes the identity authentication of Equipment A.

Subsequently, Equipment A and Equipment B use *wk* as the working key to encrypt the communication data. The working key, *wk*, is time effective, and it is eliminated according to the set timeout and the amount of encrypted data. When the use time of *wk* exceeds the set value, *wk* invalid, Equipment A and Equipment B re-authenticate and negotiate the working key. When the amount of encrypted data or encryption times by *wk* exceeds the set value, *wk* invalid, Equipment A and Equipment B re-authenticate and negotiate the working key.

5.4. V2V Secure Communication

The user private information, such as vehicle location and driving habits, may be transmitted in V2V communication; user privacy information must be protected. Moreover, the information transmitted in V2V communication may be traffic conditions, traffic

accidents, and other information related to traffic safety. Thus, it must be ensured the data transmitted in V2V communication will not be stolen, tampered, or forged, and the V2V communication is secure.

V2V secure communication should minimize the amount of calculation, save computing resources, and reduce the impact on communication delay. Thus, the V2V communication uses a symmetric algorithm and uses the working key (*wk*) negotiated in the previous authentication process.

The data encryption process is described as follows:

(1) Firstly, the hash algorithm is used to calculate the hash value of the data, and the hash value is spliced behind the data.

(2) Then, the symmetric encryption algorithm is used to encrypt the data and hash value and send the cipher data to the communication receiver.

When the C-V2X equipment receives data from other equipment, it queries the working key (*wk*) with the equipment VID and decrypts the data using the working key. If there is not a working key between the equipment, authentication negotiation is required first.

The data decryption process is described as follows:

(1) Firstly, the symmetric encryption algorithm is used to decrypt the cipher data and get the plain data.

(2) Secondly, to obtain the data and hash value from the plain data, the hash algorithm is used to calculate the hash value of the data and compares whether the calculated hash value is same with the decrypted hash value. If they are same, the decryption is successful. Otherwise, it discards the data.

6. Security Analysis and Experimental Validation

6.1. Security Analysis

This paper proposes a V2V lightweight identity authentication and key agreement scheme. The security of cryptographic protocols depends on the security strength of the cryptographic algorithms and the rigorousness of the protocol logic. With this scheme, an equipment registration center (ERC) and a key management center (KMC) are set up in the C-V2X system. Identity authentication is implemented based on identity-based cryptograph between the equipment to ensure the opposite equipment is registered equipment and the opposite equipment is trusted. During the authentication process between the equipment, the working key is synchronously negotiated and used to encrypt the communication data to ensure the confidentiality and integrity of the communication data.

Initially, the equipment registers in the ERC, obtains the VID, and obtains the private key from the KMC. The equipment send secret data encrypted with the counterpart public key to each other, verify whether the data received from the opposite equipment is the private data previously sent, implement challenge/response authentication to verify whether the identity of the opposite equipment is consistent with its VID, and confirm the opposite equipment is trusted. The private data transmitted in the authentication process can be used as the material for generating the working key, and the working key can be calculated using the agreed algorithm.

The V2V identity authentication process mainly faces two security risks: first, malicious equipment try to fake registered equipment to access the C-V2X system and try to establish secure communication with other equipment in the system. Second, malicious equipment monitor the authentication data in the open environment and try to replay the authentication response to access the system.

For the first case, the equipment generates private data, uses the opposite equipment public key to encrypt the private data, and sends the encrypted private data to the opposite equipment. The equipment verifies whether the opposite equipment has a private key consistent with its VID by verifying the opposite equipment response. Only the equipment with the private key corresponding with its VID can decrypt the encrypted private data and feedback the correct response message to verify whether the opposite equipment is registered equipment and successfully obtain the private key from the KMC.

For the second case, the authentication request and response data include the system time, *T*, and the authentication data is encrypted by the public key of the opposite equipment to ensure the *T* has not been tampered. The equipment determines whether it is replay data by verifying the effectiveness of *T*. The equipment rejects the authentication when *T* is reused or times out. When the V2V identity authentication process completes successful execution, the authentication data is invalid and cannot be reused for preventing replay attack.

The identity authentication between the equipment confirms the identity of the opposite equipment and synchronously negotiates the working key, *wk*, which used to protect the confidentiality and integrity of the communication data. The *wk* is time effective. When *wk* times out or the amount of encrypted data with the *wk* exceeds the set value, the equipment need to re-authenticate and negotiate the working key. It can ensure the working key security and prevent attacks, such as cracking the working key.

6.2. Experimental Validation

Based on the preliminary research, we establish an experimental validation environment according to the V2V identity authentication and key agreement scheme proposed in this paper. We use software to simulate the KMC which is used to generate the equipment private key according to the equipment public key. The cryptographic algorithm uses SM9. We simulated C-V2X equipment (vehicle) with a computer which installed self-developed software. The software is developed by C/C# language in the Microsoft Visual Studio environment. The experimental validation environment architecture is shown in Figure 4.

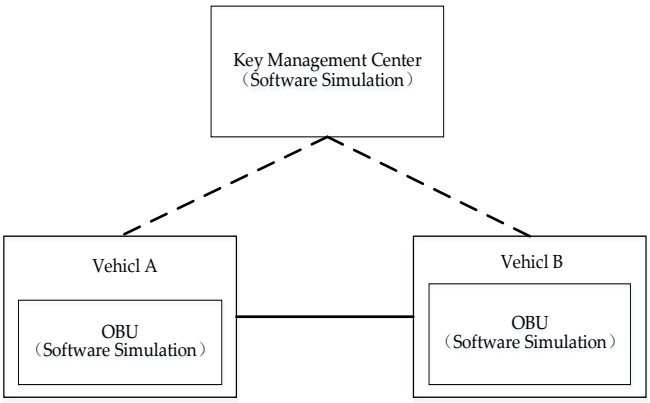

Figure 4. Experiment Environment.

The experimental process is divided into three steps: initialization process, identity authentication and key agreement process, and encryption communication process.

In the initialization phase, we first set the VIDs for Vehicle A and Vehicle B, respectively. Here, Vehicle 1 VID is "010001A0101000001000001010000 1", and Vehicle 2 VID is "010001A0101000001000002010000 1". Then, Vehicle A and Vehicle B apply for the equipment private key from the respective KMCs. The KMC calls the private key generation function (GetPrivateKey) of the SM9 algorithm, uses the VID as a parameter, and generates the private key corresponding to the VID. The KMC gives the private key to the vehicle in an internal security way (here, the private key is imported to the vehicle using offline media). The initialization of the equipment is complete.

In the identity authentication and key agreement phase, Vehicle A sends an authentication request to Vehicle B. Vehicle A generates authentication data (including random number, *r1*, system time, *T*, etc.), calls the encryption function (Encrypt) of the SM9 algorithm and uses the Vehicle B public key (*VID B*) as the encryption key to encrypt the authentication data, and sends it to Vehicle B. Vehicle B receive data from Vehicle A, calls the decryption function (Decrypt) of the SM9 algorithm and uses the Vehicle B private key (obtained from KMC and stored locally) as the decryption key to decrypt the data, and

verifies whether the time has expired. Vehicle B generates authentication data (including random number, *r2*, etc.), calls the encryption function (Encrypt) of the SM9 algorithm and uses the Vehicle A public key (*VID A*) as the encryption key to encrypt the authentication data, and sends it to Vehicle A. Vehicle A call the decryption function (Decrypt) of the SM9 algorithm and uses the Vehicle A private key (obtained from KMC and stored locally) as the decryption key to decrypt the response data, verifies whether the time has expired, obtains the authentication data, and verifies the authentication data. Vehicle A uses the authentication data to calculate the working key (*r1* XOR *r2*), calls the encryption function (Encrypt) of the SM4 algorithm and uses the working key as the encryption key to encrypt the authentication success message ("success"), and sends the message to Vehicle B. Vehicle B uses the same method to calculate the working key, decrypt the data, and obtain the authentication success message ("success"); the authentication is successful.

In the encryption communication phase, Vehicle A uses the working key with the SM4 cryptographic algorithm to encrypt the communication data and send it to Vehicle B. Vehicle B uses the working key to decrypt the data and obtain plaintext information.

The experiment simulates the identity authentication and key agreement process between the equipment and proves the scheme is effective and can be applied in the vehicle networking system. The experiment uses C/C# language to program and realize the vehicle authentication process. The authentication process simulation with software is shown in Figure 5.

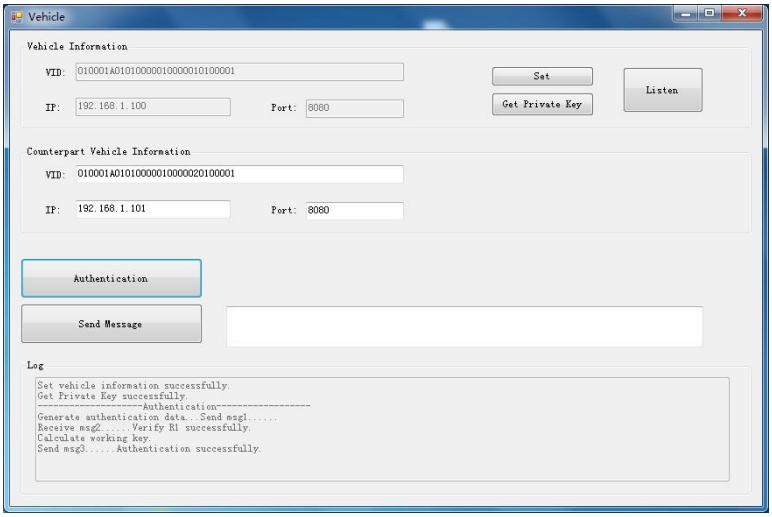

Figure 5. Authentication Process Simulation with Software.

This scheme based on identity-based cryptograph technology, uses the VID as the equipment public key, does not need to establish a CA, and does not need certificate management. The identity authentication and key agreement process only needs to transmit three data packets. We simulated this scheme identity authentication process and PKI-based identity authentication process with software. Compared with the traditional method based on the PKI system, this scheme is more lightweight and easier to implement.

7. Conclusions

This paper reviewed the C-V2X system security risks and the development of C-V2X security technology. It pointed out a low-cost and efficient authentication and encrypted communication scheme is needed in small- and medium-sized C-V2X systems. A lightweight V2V identity authentication and key agreement scheme is designed based on identity-based cryptograph technology.

The main contributions and innovations of this paper are:

(1) The scheme innovatively uses identity-based cryptograph technology in V2V communication for identity authentication with no need to establish a CA, does not need certificate management, and is lightweight and easy to implement.

(2) The C-V2X equipment interactive secret data is encrypted by a public key, verifying the response secret data, and confirms whether the opposite equipment is registered equipment, does not need to share secrets in advance between the equipment, and is convenient for deployment and application.

(3) The working key was negotiated synchronously in the identity authentication process. The scheme is convenient, efficient and has less impact on the communication delay, and is suitable for the low-delay and high-reliability requirements of the C-V2X system.

(4) The working key is used to encrypt the communication data to achieve the data confidentiality and integrity. The working key is time effective and can be changed regularly to prevent attacks on the working key.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Chen, S.; Hu, J.; Shi, Y.; Zhao, L. LTE-V: A TD-LTE-Based V2X Solution for Future Vehicular Network. *IEEE Internet Things J.* **2016**, *3*, 997–1005. [CrossRef]
2. Chen, S.; Hu, J.; Shi, Y.; Zhao, L.; Li, W. A Vision of C-V2X: Technologies, Field Testing, and Challenges with Chinese Development. *IEEE Internet Things J.* **2020**, *7*, 3872–3881. [CrossRef]
3. Alnasser, A.; Sun, H.; Jiang, J. Cyber Security Challenges and Solutions for V2X Communications: A Survey. *Comput. Netw.* **2019**, *151*, 52–67. [CrossRef]
4. Ivanov, I.; Maple, C.; Watson, T.; Lee, S. Cyber security standards and issues in V2X communications for Internet of Vehicles. In *Living in the Internet of Things: Cybersecurity of the IoT–2018*; London, UK, 2018; pp. 1–6. Available online: http://wrap.warwick.ac.uk/106474/1/WRAP-Cyber-security-standards-issues-communications-vehicles-Ivanov-2018.pdf (accessed on 17 November 2022).
5. IMT-2020(5G) Promotion Group. LTE-V2X Security Technology. Available online: http://www.IMT-2020.cn (accessed on 1 July 2019).
6. Gyawali, S.; Xu, S.; Qian, Y.; Hu, R.Q. Challenges and Solutions for Cellular Based V2X Communications. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 222–255. [CrossRef]
7. Hong, L.; Zhang, Y.; Tao, Y. Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. *IEEE Netw.* **2018**, *32*, 78–83.
8. Shin, S.; Kwon, T. A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things. *IEEE Access* **2020**, *8*, 67555–67571. [CrossRef]
9. Hakeem, S.; El-Gawad, M.; Kim, H.W. A Decentralized Lightweight Authentication and Privacy Protocol for Vehicular Networks. *IEEE Access* **2019**, *7*, 119689–119705. [CrossRef]
10. Zhang, J. Study on Secure Communication of Internet of Vehicles Based on Identity-Based Cryptograph. In Proceedings of the 2021 13th International Conference on Advanced Infocomm Technology (ICAIT), Yanji, China, 15–17 October 2021; pp. 156–160.
11. Shuhaimi, N.I.; Juhana, T. Security in vehicular ad-hoc network with Identity-Based Cryptography approach: A survey. In Proceedings of the 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), Denpasar-Bali, Indonesia, 30–31 October 2012.
12. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In Proceedings of the CRYPTO 84 on Advances in Cryptology, Santa Barbara, CA, USA, 23 August 1985; Available online: https://dl.acm.org/doi/10.5555/19478.19483 (accessed on 17 November 2022).
13. Gallegos-Garcia, G.; Gomez-Cardenas, R.; Duchen-Sanchez, G.I. Electronic Voting Using Identity Based Cryptography. *Sci. World J.* **2015**, *2015*, 741031. [CrossRef]
14. Tian, C.; Wang, L.; Li, M. Design and Implementation of SM9 Identity Based Cryptograph Algorithm. In Proceedings of the 2020 International Conference on Computer Network, Electronic and Automation (ICCNEA), Xi'an, China, 25–27 September 2020; pp. 96–100.
15. Cryptography Standardization Technical Committee. Information Security Technology—Identity-Based Cryptographic Algorithms SM9—Part 1: General. Available online: http://www.gmbz.org.cn (accessed on 1 November 2020).

16. Li, H.; Sun, S. Identity-Based Cryptography for Grid. In Proceedings of the Eighth Acis International Conference on Software Engineering, Qingdao, China, 30 July–1 August 2007.
17. Chen, S.; Li, Q.; Wang, Y.; Xu, H.; Jia, X. C-V2X equipment identification management and authentication mechanism. *China Commun.* **2021**, *18*, 297–306. [CrossRef]