Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.038029
Article

Secure Blockchain-Enabled Internet of Vehicles Scheme with Privacy Protection

Jiansheng Zhang[1], Yang Xin[1,*], Yuyan Wang[2], Xiaohui Lei[2] and Yixian Yang[1]

[1]Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2]Beijing Everyone Crowdsourcing Technology Company Ltd., Beijing, 100018, China
*Corresponding Author: Yang Xin. Email: yangxin@bupt.edu.cn
Received: 24 November 2022; Accepted: 08 February 2023

Abstract: The car-hailing platform based on Internet of Vehicles (IoV) technology greatly facilitates passengers' daily car-hailing, enabling drivers to obtain orders more efficiently and obtain more significant benefits. However, to match the driver closest to the passenger, it is often necessary to process the location information of the passenger and driver, which poses a considerable threat to privacy disclosure to the passenger and driver. Targeting these issues, in this paper, by combining blockchain and Paillier homomorphic encryption algorithm, we design a secure blockchain-enabled IoV scheme with privacy protection for online car-hailing. In this scheme, firstly, we propose an encryption scheme based on the lattice. Thus, the location information of passengers and drivers is encrypted in this system. Secondly, by introducing Paillier homomorphic encryption algorithm, the location matching of passengers and drivers is carried out in the ciphertext state to protect their location privacy. At last, blockchain technology is used to record the transactions in online car-hailing, which can provide a security guarantee for passengers and drivers. And we further analyze the security and performance of this scheme. Compared with other schemes, the experimental results show that the proposed scheme can protect the user's location privacy and have a better performance.

Keywords: Blockchain; IoV; privacy protection; anti-quantum

1 Introduction

In the Internet of vehicles (IoV), vehicles use onboard communication equipment to conduct wireless communication and information exchange through specific protocols and data standards to realize network interconnection with other vehicles, road facilities and service management platforms [1]. The connection realizes the control of intelligent vehicles and intelligent transportation. And it provides many convenient and diversified services for intelligent transportation [2,3]. Through the IoV, ordinary users and drivers can quickly obtain safe, advanced and comfortable services. The rapid development of IoV technology has fundamentally changed people's production and life [4].

For example, under the trend of the Internet-sharing economy, online car-hailing service based on vehicle networking has developed rapidly, which not only facilitates the car-hailing travel of users but also improves the efficiency of online car-hailing service.

However, due to the need for multiple message exchanges between vehicle and vehicle networking systems, IoV is facing the challenge of privacy leakage. Taking the parking charging service in IoV of smart city as an example, when users register and pay for parking to the service provider, many privacy information of users, such as hobbies, vehicle information, location and habits, will be obtained by the service provider. In this process, how to protect users' privacy has become the key [5,6]. Therefore, while providing services, the IoV needs to focus on the design of a privacy protection model. Users can not only enjoy high-quality services but also avoid their private information being illegally obtained by a third party [7], which needs to find a solution to protect the privacy information of vehicles and users.

Nakamoto proposed a new decentralized digital currency based on blockchain technology [8,9]. Nowadays, the success of the bitcoin case has proven the strong development potential and application value of blockchain technology. Blockchain can share a secure public database through the distributed network without trust between users [10].

Due to the large amount of real-time data generated in IoV, these data enrich the context and social relationship information of vehicles, drivers, passengers and the surrounding environment. The data are collected and stored in different layers of its architecture. Therefore, the role of privacy management in IoV becomes crucial [11]. With the characteristics of decentralization and independence, emerging blockchain is widely used in finance, providing a new way to solve the privacy disclosure in the IoV. In 2018, Arora et al. proposed a method to provide authentication and secure data transmission between vehicle nodes in IoV to ensure accurate information communication between nodes [12]. However, the proposed algorithm is not analyzed and verified in this paper. Based on blockchain technology, Knirsch et al. proposed a protocol to match the most cost-effective charging station near the vehicle without disclosing the location information of electric vehicles [13]. Electric vehicles send demand signal, and charging stations can send bids similar to an auction. The principle of this scheme is relatively simple, but the protocol requires multiple communications during the process, which has the disadvantage of high communication costs. Xu et al. proposed a blockchain-based data-sharing framework to adapt to the limited computing and storage resources in edge devices [14]. Recently, in 2020, the authors in Ref. [15] proposed a collaborative data sharing model for industrial IoT applications, in which data owners and data requesters can achieve secure and fast data exchange between decentralized parties. In 2021, Qi et al. proposed a consortium blockchain-based federated learning framework, which can protect data privacy in industrial Internet by applying a noise-adding mechanism for the blockchain-based federated learning framework [16]. In this study, miners can verify model updates to avoid fraudulent updates, thereby mitigating the impact of data poisoning attacks. In addition, differential privacy has been used to prevent inference attacks and protect vehicle privacy. Unfortunately, with the increasing number of customers, the vast data processing and storage will become a new challenge for this framework to be further optimized.

Taking advantage of the decentralized, anonymous, and tamper-proof characteristics, blockchain can bring a new decentralized solution to the privacy disclosure problem of the IoV data, which is conducive to enhancing the safe data-sharing. At the same time, the blockchain does not need a trusted environment and special hardware facilities. It can combine multiple devices at the network's edge to achieve secure and reliable data consensus, reducing communication and hardware costs. More importantly, combining the IoV and blockchain technology can also form a trustworthy computing and effective incentive mechanism. Therefore, introducing blockchain into the IoV system ensures

data privacy and security, which is of great significance for promoting data sharing of the Internet of Vehicles.

Blockchain has promoted the development of IoV from centralized to distributed trust mode, and Blockchain-enabled Internet of Vehicles (BIoV) is proposed. Aiming at the challenges of privacy protection and data security, we propose a location privacy protection method based on homomorphic encryption and blockchain. This method requires each passenger and driver to encrypt their location information before issuing a request, and then send the ciphertext to the online car-hailing platform. The car-hailing platform uses homomorphic encryption technology to execute the user's location.

The remainder of this paper is organized as follows. In Section 2, we make a brief introduction to related works, security model, and paillier homomorphic encryption. In Section 3, an asymmetric encryption scheme is proposed. Afterward, the privacy protection scheme for BIoV is designed. In Section 4, we further illustrate and analyze its security, and we compare the performance of our scheme in Section 5. At last, some concluding remarks are presented in Section 6.

2 Preliminary

2.1 Related Works

For vehicle positioning, the IoV mainly adopts location-based service (LBS). In LBS, private car first provides services to LBS providers (LBSP, location-based service provider). It sends a query request message, including the current vehicle location and query keywords that can reflect the vehicle interest. Then, LBSP returns a keyword-based response message, including a Point of Interest (PoI) related to the vehicle location and query keywords, such as restaurants, gas stations, and parking lots.

Although LBS brings many benefits and convenience to users, it also has the problem of privacy disclosure. For example, when the location data is leaked, the enemy can reconstruct its driving track and infer the private information of the vehicle user, such as a home address, work unit, and health status. The disclosure of this private information may lead to acts endangering the user's safety [17]. Therefore, location privacy protection in LBS has attracted the attention of scholars. Because of the above problems, there are mainly three types of solutions.

(1) Using the cryptographic algorithms to provide privacy protection. The representative achievement is that Yi et al. [18] proposed a location privacy protection scheme based on differential privacy, which uses Paillier homomorphic encryption technology to realize geographic indistinguishable s-differential location privacy. Paulet et al. [19] proposed a nearest-neighbor search scheme. In 2021, Yi et al. designed a privacy protection scheme using the ring signature algorithm on the lattice [20].

(2) Use confusion strategies. Beresford et al. [21] proposed the concept of diverse region and introduced the idea of confusion in location privacy protection. The principle is to constantly change the user's pseudonym in this area to protect the user's location privacy. In 2017, Yang et al. Proposed a new method that can completely protect the user's location privacy, the confined space hiding method [22].

(3) Using space and pseudonyms. Users can retrieve the required content in the local cache without sending queries to LBSP, which protects privacy. For example, Amini's scheme [23] and Shokri et al. [24]. In 2018, Khodaei et al. Proposed a collaborative location privacy protection scheme to hide the location information of vehicles [25].

2.2 Security Model

According to the description of privacy attacks in Ref. [26], the security modes are divided into the following types.

(1) IoV location privacy disclosure. By attacking the vehicle networking system data, the attacker may obtain the location data or travel trajectory of the driver or passenger, expose the specific location, and disclose the personal privacy information of the driver and passenger users.

(2) Blockchain data disclosure. As is known to all, blockchain is open and transparent. Other users can also read the driving record information in the blockchain ledger. Therefore, potential attackers can read all transactions recorded on the blockchain to gain the privacy of passengers and drivers.

(3) Payment fraud. If the driver is paid at the beginning of the trip, he may not be able to complete the trip. In addition, if the driver receives the fare at the end of the trip, the passenger may not be willing to pay the fare.

2.3 Paillier Homomorphic Encryption

Homomorphic encryption is a special encryption method. In addition to the particular encryption operation, it can also realize various computing functions between ciphertext. Various mathematical calculation operations are carried out for ciphertext, and the results of these operations are the same as those on plaintext [8]. In other words, homomorphic encryption allows specific calculations to be performed on the encrypted data without knowing the private key. And the decrypted result of the encrypted data obtained after the calculation is the same as that obtained by performing the same calculation on the plaintext. The implementation effect is shown in Fig. 1, and homomorphic encryption algorithm is often used to protect data privacy.

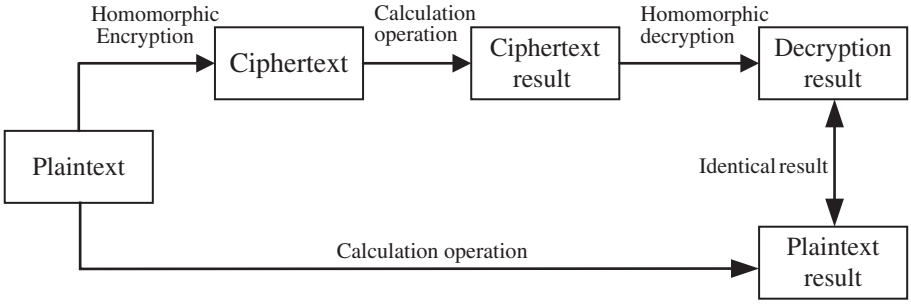

Figure 1: Homomorphic encryption

The Paillier algorithm is one of the most studied homomorphic encryption algorithms. The details of the Paillier algorithm are as follows.

Key generation. Select two large primes p and q, which satisfies the following equation

$$\gcd(pq, (p-1)(q-1)) = 1. \tag{1}$$

Then calculate

$$n = pq, \tag{2}$$

$$\lambda = lcm(p-1, q-1). \tag{3}$$

The *lcm* function is used to calculate the least common multiple of the two parameters.

Select a random integer $g \in Z_{n^2}^*$, and g satisfies

$$\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n. \tag{4}$$

$L(u)$ is defined as $L(u) = (u-1)/n$. $Z_{n^2}^*$ represents the set of integers coprime to n^2 in Z_{n^2}. Thus, the user obtains the public and private keys that can be used for homomorphic encryption. The public key is (n, g) and the private key is λ.

Encryption. Suppose that the information m needs to be encrypted and $m \in Z_n, 0 < m < n$. Randomly select an integer $r \in Z_{n^2}^*$ and $r < n$. The encryption algorithm as $c = E(m, r)$. Calculate and obtain the ciphertext

$$c = E(m, n, g) = g^m r^n \bmod n^2. \tag{5}$$

Decryption. For the ciphertext c, calculate as follows and obtain the plaintext m.

$$m = D(c) = L\left(c^{\lambda} \bmod n^2\right) \mu \bmod n = \frac{L\left(c^{\lambda} \bmod n^2\right)}{L\left(g^{\lambda} \bmod n^2\right)} \bmod n. \tag{6}$$

3 BIoV with Privacy Protection

3.1 Architecture of the BIoV

The architecture of the BIoV is described in Fig. 2 below. The management of vehicle data is realized through a five-layer structure which includes the physical layer, network layer, consensus layer, platform layer, and application layer. The detail function introductions of every layer are as follows.

(1) **Physical layer.** This layer is mainly the intelligent devices in the IoV, such as intelligent vehicles and Roadside Units (RSU). As the edge computing infrastructure of BIoV, RSU is widely deployed in the whole road network. Therefore, vehicles can easily reach the range of RSU receiving data. Because these RSUs have sufficient computing and storage resources, they can become miners in blockchain technology to collect and record driving data for the BIoV. Therefore, these miners play an important role in publicly reviewing and storing vehicle data and data-sharing records in BIoV.

(2) **Network layer.** The network layer mainly changes the protocols related to the communication between nodes, such as Bluetooth, WiFi, ZigBee and other network protocols. Blockchain network is a distributed network in which user nodes broadcast transactions to other user nodes it knows in the network. If the core user node in the network receives the transaction, first verify whether the signature in the transaction is correct, whether the transaction structure is correct, and whether the size is within the specified range. If all validations are successful, the transaction will be further aggregated and added to the new block.

(3) **Consensus layer.** The consensus layer mainly includes RSU and blockchain systems in the IoV. The consensus mechanism is one of the core technologies of blockchain, which determines whose block will be the next block of the main chain in a decentralized and trusting environment. The purpose of the consensus layer is to realize the consensus and unification of the node storage ledger in a distributed network. In BIoV, each RSU can be regarded as a miner node in the blockchain system. The data is sorted and uploaded to the blockchain system through the RSU.

The blockchain system adopts the Delegated Proof of Stake (DPoS). It adopts the method of electing principal, who as a producer of the new block in turn. Unlike the previous Proof of Work (PoW) mining methods, this method not only reduces the energy consumption of the blockchain system and minimizes the network operation cost, but also improves the block confirmation time.

The evaluation confirmation time of each block is about 10 s. The above advantages make DPoS more suitable for IoV applications.

(4) **Platform layer.** As shown in Fig. 2, the device layer is mainly the intelligent devices that drivers, passengers access and use vehicle data, such as mobile phones and computers. Through these devices, users can connect with the BIoV system through the network. Thus, the BIoV system can provide users with various transportation services efficiently and conveniently.

(5) **Application layer.** The application layer is the highest level of the BIoV system which is mainly applicable to the application scenarios of blockchain. According to different application scenarios, the application layer will also be different. Based on the safety of the BIoV model, it can be applied to car-hailing, intelligent transportation and other application scenarios.

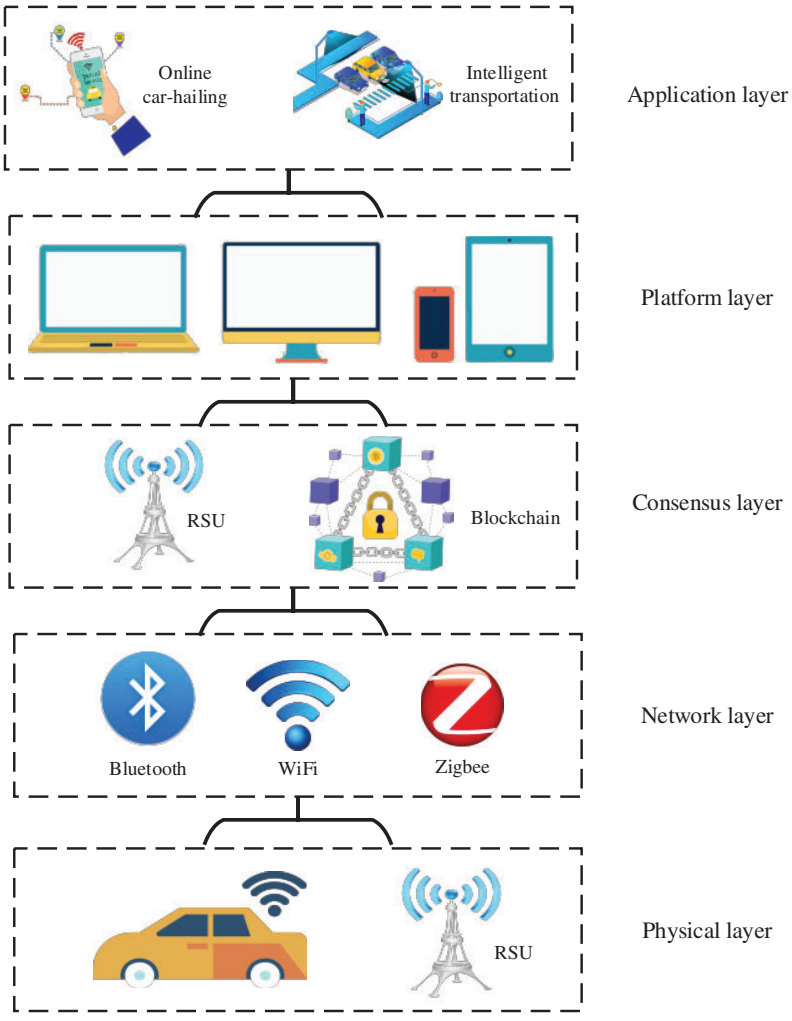

Figure 2: The architecture of BIoV

3.2 Lattice-Based Encryption Scheme

In this subsection, we propose an encryption scheme based on lattice as follows. For one thing, we introduce two lemmas used in the scheme. For another, we describe the encryption and decryption process of the scheme in detail. Our scheme consists of four probabilistic polynomial time (PPT) algorithms.

Lemma 1. *TrapGen* (q, n). Given a prime $q \geq 2$, $\{n, m\} \in Z, m \geq 5n \log q$. Run *TrapGen* (q, n) algorithm can output $A \in Z_q^{n \times m}$ and $S_A \in Z_q^{m \times m}$, where S_A is a basis for $L_q^{\perp}(A)$ satisfying $\left|\left|\widetilde{S}_A\right|\right| \leq O\left(\sqrt{n \log q}\right)$ and $||S_A|| \leq O(n \log q)$.

Lemma 2. *SampleLeft* (A, B, S_A, u, σ). Input $A \in Z_q^{n \times m}$, $B \in Z_q^{n \times m_1}$, $S_A \in Z_q^{m \times m}$, a vector $u \in Z_q^n$ and a Gaussian parameter $\sigma \geq ||S_A|| \omega\left(\sqrt{\log(m + m_1)}\right)$, run *SampleLeft* (A, B, S_A, u, σ) algorithm can output a vector $e \in L_q^u(F)$ and $F = (A|B) \in Z_q^{n \times (m+m_1)}$ satisfying $Fe = u \bmod q$.

Setup. Select two primes n, $q \geq 2$, and an integer $m \geq 5n \lg q$, which are security parameters in this scheme. Then, run $(P, S) \leftarrow TrapGen(1^n), P \in Z_q^{n \times m}$ and output the public key $PK = P$, master key $MK = S$.

Key generation. Choose a matrix $b \in Z_q^{n \times m}$ randomly and a parameter $\sigma \geq ||S|| \omega(\text{lb}m) \sqrt{m}$. Input the Public key P and master key S and run *SampleLeft*(P, k_i, S, b, σ) to output s_i. Thus, system generates secret key $sk = (s_i, b)$.

Encryption. Choose error parameter $a \leftarrow \chi$, where χ is Gaussian error distribution. Plaintext $\text{M} = m_x \in \{0, 1\}$, compute $c_1 = a + m_x \lfloor q/2 \rfloor$. Then, select $x \in Z_q^m \leftarrow \chi$ and $d \in \{-1, 1\}^{m \times m}$ randomly. Compute $c_2 = dx$ and output the ciphertext $C = \{c_1, c_2\}$.

Decryption. The algorithm takes the public key, private key sk and ciphertext C as inputs. Compute

$w = s_i c_2 = s_i dx$,

$g = c_1 - w$

If $|g - \lfloor q/2 \rfloor| < \lfloor q/4 \rfloor$, return $m_x = 1$. Else, return $m_x = 0$, thus, plaintext M is obtained.

3.3 Privacy Protection for BIoV

The decentralized BIoV system proposed in this section eliminates the intermediary mechanism in the current online car-hailing service system. A decentralized Internet of vehicles service system is constructed by using blockchain technology and smart contract. The security requirement in this system is to protect the location privacy of taxi users. Therefore, we assume that the system contains four key nodes.

As mentioned above, the Paillier algorithm is a homomorphic encryption algorithm. The positions of passenger and driver are represented by loc_p and loc_d, respectively. As shown in Fig. 3, the detail steps of privacy protection for BIoV are as follows.

Step 1. Key generation. The cryptographic service system runs the Paillier algorithm to obtain the public key and private key (pkh, skh). Meanwhile, it runs the proposed lattice-based asymmetric encryption scheme to generate public-private key pairs for each passenger and driver. In general, (pk_p, sk_p) and (pk_d, sk_d) are used to denote the public-private key pairs for passenger and driver respectively. (pk_c, sk_c) represents the system's public-private key pair.

Step 2. Encryption. Suppose that the number of drivers is x, thus, there is a driver's location set $D = \{loc_{d1}, loc_{d2}, \ldots, loc_{d(x-1)}, loc_{dx}\}$. The process of encrypting passenger and driver location information is as follows.

(1) The passenger's current position and driver's location set $D = \{loc_{d1}, \ldots, loc_{dx}\}$ are encrypted by the system's public key and sent to the cryptographic service system.

(2) Service system decrypts the location information of passenger and drivers through its private key sk_c.

(3) Through Paillier algorithm, the public key pkh is used to encrypt the position information of passenger and drivers

$$c_p = E(loc_p, pkh),\ c_{di} = E(loc_{di}, pkh),\ i \in [1, x]. \tag{7}$$

And the generated ciphertext c_p and c_{di} are sent to the BIoV.

Step 3. Homomorphic calculation. The BIoV system receives the position information ciphertext of passenger and drivers. It combines the road network embedding algorithm to calculate the homomorphism of position information in high-dimensional spatial coordinates to obtain the linear ciphertext distance d_i between passengers and drivers as follows.

$$d_i = dist(c_p + c_{di}), i \in [1, x]. \tag{8}$$

Afterward, the BIoV returns these ciphertext information results to the cryptographic service system.

Step 4. Matching request. The driver retrieves and selects the passenger's boarding request from the blockchain network, encrypts the passenger's location, and sends a message to the blockchain to accept the request for additional public key. The passenger encrypts the specific riding position using the public key of the driver receiving the trip, and sends the encrypted position to the blockchain.

Step 5. Get private address. After the driver gets it back, decrypt the passenger's specific location, and then drive to pick up the passenger.

Step 6. Blockchain transaction. When the driver arrives at the designated location after decryption, the passenger will inform the driver of the destination. The driver encrypts the destination with the passenger's public key and sends the ciphertext to the blockchain.

Step 7. Complete transaction. The passenger releases a transaction information to upload to the blockchain, pays in advance and starts taking the bus. Based on the smart contract, when the conditions for arriving at the destination are met, passengers need to release the end of journey message to the blockchain. The smart contract will automatically calculate the driver's commission and transfer it to the driver's account.

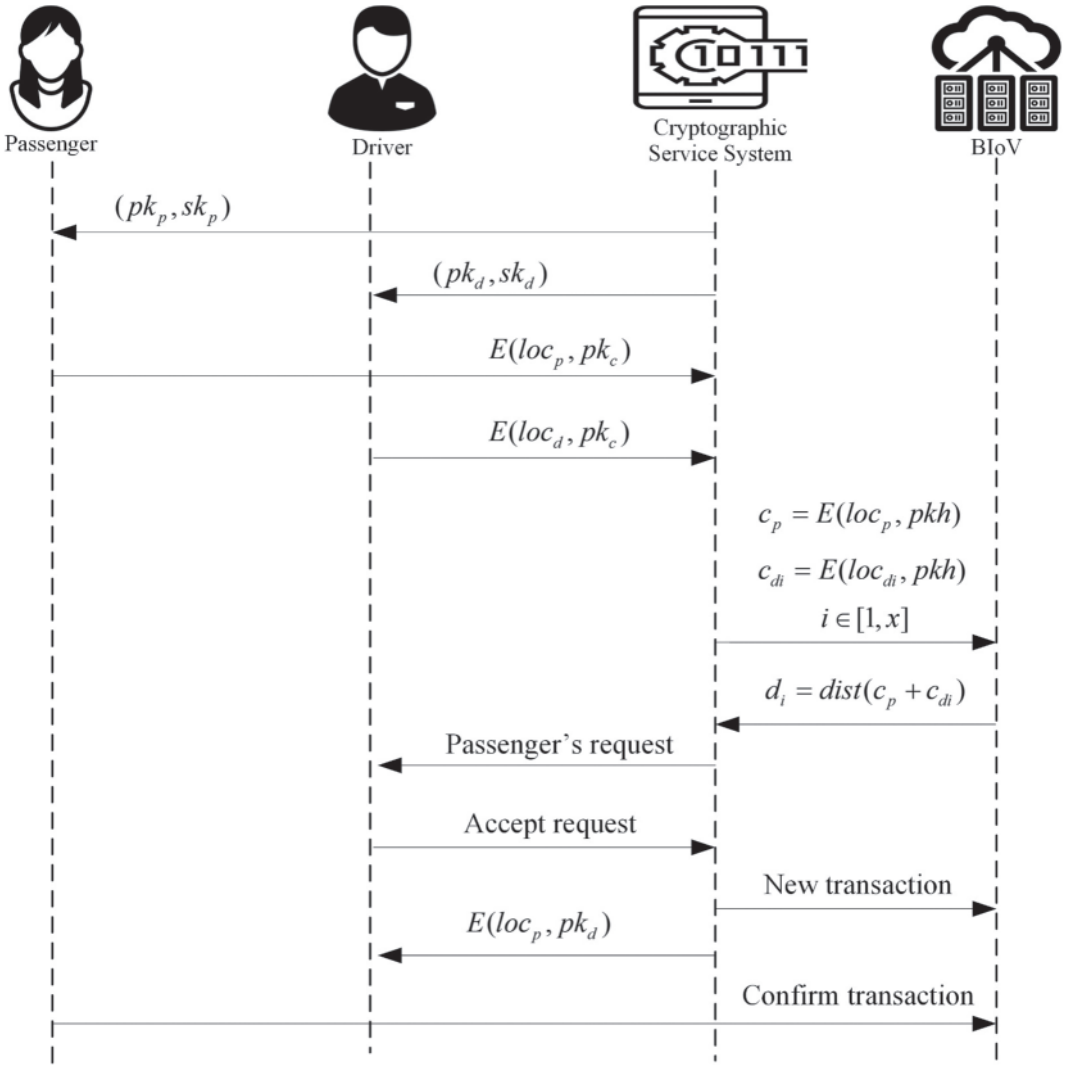

Figure 3: The processes of anonymity authentication for BIoV

4 Security Analysis

4.1 Correctness

Theorem 1. Using the encryption algorithm to encrypt plaintext M, the decryption algorithm decrypts plaintext M with a probability close to 1.

In the decryption phase of the lattice scheme, $w = s_i c_2 = s_i dx$, $g = c_1 - w$. So we can have

$$\begin{aligned} g &= c_1 - w \\ &= a + m_x \lfloor q/2 \rfloor - s_i dx. \end{aligned} \tag{9}$$

In particular, the parameters a and $s_i dx$ are short vectors in this scheme, therefore, the result $a - s_i dx$ will be in $(-q/4, q/4)$. As the above Eq. (9) holds, we can derive that $\left\lfloor \frac{a + m_x \lfloor q/2 \rfloor - s_i dx}{\lfloor q/2 \rfloor} \right\rceil = m_x$. Therefore, the decryption algorithm can decrypt the ciphertext and obtain the plaintext M.

4.2 Privacy Security

Our scheme mainly serves the location information of passengers and drivers through the communication between the cryptographic service system and the IoV. More specifically, the cryptographic service system encrypts the location information and then sends it to the IoV to calculate the ciphertext. Finally, the service system decrypts the ciphertext results to obtain the distance between the driver and passengers. Then it generates the transaction between the driver and passengers through the blockchain to complete the taxi service. In IoV, the location information of drivers and passengers is encrypted. Therefore, the IoV can not obtain the user's address information, which ensures the user's location privacy.

Proof. Homomorphic encryption is a particular form of encryption which allows people to calculate the encrypted data without decrypting it. The calculation result is also presented in encryption, and the output after decryption is the same as that obtained by processing unencrypted data in the same method. Based on the homomorphism of the Paillier public key cryptosystem, the correctness of the location information calculation in the scheme is proved as follows.

Decryption. For the ciphertext c, calculate as follows and obtain the plaintext m.

$$m = L\left(c^{\lambda} \bmod n^2\right) \mu \bmod n = \frac{L\left(c^{\lambda} \bmod n^2\right)}{L\left(g^{\lambda} \bmod n^2\right)} \bmod n. \tag{10}$$

Additive homomorphism. For the plaintext m_1 and m_2, the result of encryption is

$$c_1 = g^{m_1} r_1^n \bmod n^2,\ c_2 = g^{m_2} r_1^n \bmod n^2. \tag{11}$$

Therefore, we can get the following equation

$$c = c_1 \cdot c_2 = g^{m_1+m_2} (r_1 r_2)^n \bmod n^2. \tag{12}$$

The ciphertext c can be decrypted as

$$m = \frac{L\left(c^{\lambda} \bmod n^2\right)}{L\left(g^{\lambda} \bmod n^2\right)} \bmod n = m_1 + m_2. \tag{13}$$

In this way, even if the location information of passengers and drivers is in the ciphertext state, IoV can obtain correct results and provide them with complementary taxi services as before. The homomorphic encryption ensures the security of users' location privacy information in the IoV.

4.3 Attack Resistance

The location privacy disclosure of passengers and drivers has always been one of the essential research contents of IoV security. In this subsection, we will analyze these attack modes and verify the security of our scheme.

(1) Resistance IoV location privacy disclosure.

For the privacy disclosure of the IoV, we introduce homomorphic encryption in it. Therefore, all the location information obtained by the IoV is encrypted ciphertext information. On the one hand, without knowing Paillier's private key, IoV can't know the specific location of passengers and drivers, nor can it get their driving route. It shows that our scheme can ensure the location privacy and security of users. On the other hand, the Paillier encryption algorithm satisfies additive homomorphism, ciphertext multiplication is equal to plaintext addition. Therefore, after the encrypted location information is calculated, the distance result is not only presented in the form of ciphertext, but also the decrypted result is the same as that obtained with the corresponding calculated plaintext data. Therefore, our scheme can resist location privacy disclosure in BIoV.

(2) Resistance to blockchain data disclosure.

Blockchain is open and transparent. Anyone can read the driving record information in the blockchain ledger. However, in our blockchain transaction information, the transaction sheet mainly includes the wallet, signature and numbers of passengers and drivers. It does not include the location information of passengers and drivers. Therefore, in our proposed scheme, the information on the blockchain will not disclose the location information of passengers and drivers.

(3) Resistance payment fraud.

For the payment fraud problem caused by the lack of trust of passengers and drivers, it can be optimized and improved through the blockchain technology in the proposed scheme. On the blockchain platform, there is a passenger's wallet account. After the driver accepts the passenger's ride order, the transaction order begins to be created. Before arriving at the destination, without the passenger's signature on the transaction, the driver can not obtain income, avoiding the situation that the driver does not complete the taxi service when he is paid. When the driver arrives at the designated destination, the smart contract of the blockchain can provide a proof for this transaction and prompt the passengers to complete this transaction. Therefore, the problem of ticket evasion can be avoided.

5 Comparison

Generally speaking, the size of the secret key is essential to the encryption scheme's performance in practical applications. Compared with other algorithms in Ref. [27], Ref. [28] and Ref. [29]. As shown in Table 1, the sizes of the public key and private key in other schemes are larger than those in our scheme. In addition, the security of the signature algorithm in this paper depends on the lattice SIS problem. As we know, the lattice SIS problem in the average case can be reduced to the shortest independent vector problem (SIVP) in the worst case in polynomial time. It shows that our scheme is more secure and effective.

Table 1: Performance comparison with other similar schemes

Scheme	Public key size	Private key size
Ref. [27]	$mn\log(2q+1)$	$mn\log(2q+1)$
Ref. [28]	$(mn+dm)\log q$	$m^2\log q$
Ref. [29]	$Mn\log q$	$m^2\log q$
Our scheme	$Mn\log q$	$(m+mn)\log q$

According to the actual requirements in these schemes, under reasonable parameters $d = \lceil \log n \rceil$, $q = 2^{10}$, $m = 6n\log q$, take the range of security parameter n to increase from 10 to 160. The public key size and private size of our proposed scheme and those in Ref. [27], Ref. [28] and Ref. [29] are compared respectively. And the simulation experiment results are shown in Figs. 4 and 5, respectively. Obviously, with the security parameter n's increase, the public key and private key sizes in our lattice-based scheme are significantly reduced, which can improve operational efficiency in the BIoV scheme with privacy protection.

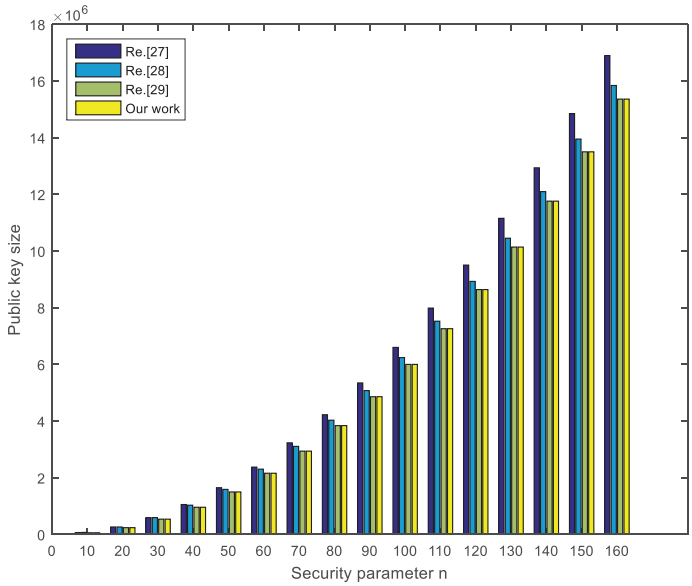

Figure 4: The public key size comparison

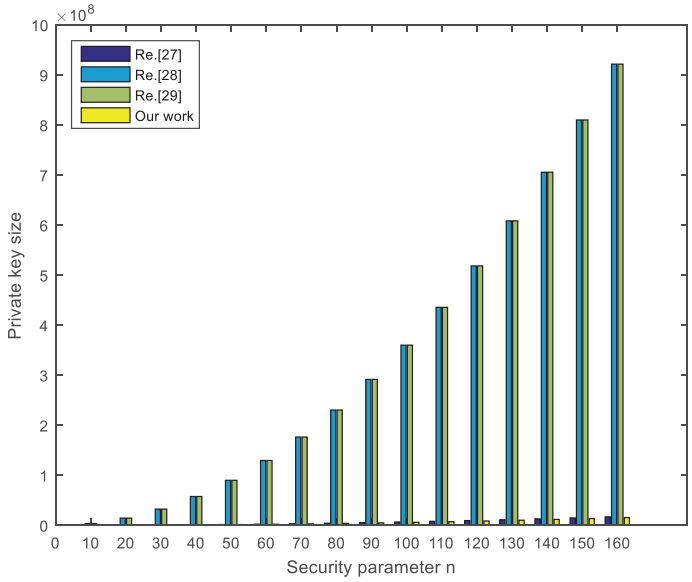

Figure 5: The private key size comparison

6 Conclusions

The IoV is a network that provides efficient and safe information services by building a network topology between vehicles, pedestrians, roadside units, and other communication entities. The IoV can effectively meet the growing demand for traffic environment. However, because of its mobility and openness, the IoV is vulnerable to attacks. Among the numerous threats, the privacy disclosure of IoV users may cause irreparable losses, so the privacy protection of IoV is widely concerned by researchers. In this paper, we conduct research on the privacy protection for IoV and introduce the current relevant research results. Targeting this issue, we propose a lattice-based encryption scheme. Thus, the location information of passengers and drivers can be encrypted with anti-quantum security. Then, by introducing Paillier homomorphic encryption algorithm, the location matching of passengers and drivers is carried out in the ciphertext state to protect their location privacy. At last, blockchain is used to record the transactions in online car-hailing, which can provide a security guarantee for passengers and drivers. And we further analyze the security and performance of this scheme. Compared with other schemes, the experimental results show that the proposed scheme can protect the user's location privacy and have a better performance. Our study in this paper mainly aims at the data security problem of the IoV system, especially the privacy leakage problem, and proposes new solutions to provide theoretical support for the construction of future IoV data privacy protection. Researchers can further study this promising technology in IoV security. In future research, we will also further explore the performance optimization for the IoV privacy protection scheme.

Acknowledgement: The authors are grateful to the financial supports from the National Key R&D Program of China, Major Scientific and Technological Special Project of Guizhou Province, the Foundation of Guizhou Provincial Key Laboratory of Public Big Data, and the Fundamental Research Funds for the Central Universities.

Funding Statement: This work is supported by National Key R&D Program of China (Grant No. 2020YFB1805403), Major Scientific and Technological Special Project of Guizhou Province (Grant No. 20183001), Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant Nos. 2018BDKFJJ021, 2018BDKFJJ020, 2017BDKFJJ015, 2018BDKFJJ008), the Fundamental Research Funds for the Central Universities (CUC210A003).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Contreras, S. Zeadally and J. A. Guerrero-Ibanez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[2] F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun, "An overview of internet of vehicles," *China Communications*, vol. 11, no. 10, pp. 1–15, 2014.

[3] M. Gerla, E. K. Lee, G. Pau and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. of the 2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, Korea, pp. 241–246, 2014.

[4] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao *et al.,* "Routing in internet of vehicles: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[5] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang *et al.,* "Security and privacy in the internet of vehicles," in *Proc. of the 2015 Int. Conf. on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, Beijing, China, pp. 116–121, 2015.

[6] Q. Kong, R. Lu, M. Ma and H. Bao, "A privacy-preserving sensory data sharing scheme in internet of vehicles," *Future Generation Computer Systems*, vol. 92, pp. 644–655, 2019.
[7] T. Wang, Z. Cao, S. Wang, J. Wang, L. Qi *et al.,* "Privacy-enhanced data collection based on deep learning for internet of vehicles," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6663–6672, 2019.
[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[9] M. Hamilton, "Blockchain distributed ledger technology: An introduction and focus on smart contracts," *Journal of Corporate Accounting and Finance*, vol. 31, no. 2, pp. 7–12, 2020.
[10] G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. of the 2015 IEEE Security and Privacy Workshops*, San Jose, CA, pp. 180–184, 2015.
[11] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily and Y. Jararweh, "Privacy management in social internet of vehicles: Review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019.
[12] A. Arora and S. K. Yadav, "Block chain based security mechanism for internet of vehicles (iov)," in *Proc. of the 3rd Int. Conf. on Internet of Things and Connected Technologies (ICIoTCT)*, Jaipur, India, pp. 26–27, 2018.
[13] F. Knirsch, A. Unterweger and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science-Research and Development*, vol. 33, no. 1, pp. 71–79, 2018.
[14] C. Xu, K. Wang, G. Xu, P. Li, S. Guo *et al.,* "Making big data open in collaborative edges: A blockchain-based framework with reduced resource requirements," in *Proc. of the 2018 IEEE Int. Conf. on Communications (ICC)*, Kansas City, MO, USA, pp. 1–6, 2018.
[15] Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2019.
[16] Y. Qi, H. S. Hossain, J. Nie and X. Li, "Privacy-preserving blockchain-based federated learning for traffic flow prediction," *Future Generation Computer Systems*, vol. 117, pp. 328–337, 2021.
[17] L. Hu, Y. Qian, M. Chen, M. S. Hossain and G. Muhammad, "Proactive cache-based location privacy preserving for vehicle networks," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 77–83, 2018.
[18] X. Yi, R. Paulet, E. Bertino and V. Varadharajan, "Practical k nearest neighbor queries with location privacy," in *Proc. of the 2014 IEEE 30th Int. Conf. on Data Engineering*, Chicago, IL, USA, pp. 640–651, 2014.
[19] R. Paulet, M. G. Kaosar, X. Yi and E. Bertino, "Privacy-preserving and content-protecting location based queries," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1200–1210, 2014.
[20] H. Yi, "Secure social internet of things based on post-quantum blockchain," *IEEE Transactions on Network Science and Engineering*, 2021. https://doi.org/10.1109/TNSE.2021.3095192
[21] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.
[22] G. Yang and Y. Cai, "Full location privacy protection through restricted space cloaking," *Journal of Information Processing*, vol. 25, pp. 756–765, 2017.
[23] S. Amini, J. Lindqvist, J. Hong, J. Lin, E. Toch *et al.,* "Caché: Caching location-enhanced content to improve user privacy," in *Proc. of the 9th Int. Conf. on Mobile Systems, Applications, and Services*, New York, USA, pp. 197–210, 2011.
[24] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi and J. P. Hubaux, "Hiding in the mobile crowd: Location privacy through collaboration," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 3, pp. 266–279, 2013.
[25] M. Khodaei and P. Papadimitratos, "Poster: Mix-zones everywhere: A dynamic cooperative location privacy protection scheme," in *Proc. of the 2018 IEEE Vehicular Networking Conf. (VNC)*, Taipei, Taiwan, pp. 1–2, 2018.
[26] M. Li, L. Zhu and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4573–4584, 2019.

[27] M. Ruckert, "Lattice-based blind signatures," in *Proc. of the Int. Conf. on the Theory and Application of Cryptology and Information Security*, Berlin, Heidelberg, pp. 413–430, 2010.
[28] L. Zhang and Y. Ma, "A lattice-based identity-based proxy blind signature scheme in the standard model," *Mathematical Problems in Engineering*, vol. 2014, pp. 1–6, 2014.
[29] C. Li, X. Chen, Y. Chen, Y. Hou and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2019.