The Latticed-Based Path Privacy Protection Aggregation Scheme for Internet of Vehicles

CHENG WEI1, TAO WU1, XINGYU LIU1, AND SHUO XIONG2

1School of Software, Huazhong University of Science and Technology, Wuhan 430074, China
2School of Journalism and Information Communication, Huazhong University of Science and Technology, Wuhan 430074, China

Corresponding author: Tao Wu (wutao1972@hust.edu.cn)

This work was supported by the Natural Science Foundation of China under Grant 51575204 and Grant 52175536.

ABSTRACT With the occurrence of information leakage events of online ride-hailing, the information security of Internet of Vehicles has been highly valued by the society. Once the information of the Internet of Vehicles is exposed by the online ride-hailing platform or stolen by hackers, it will pose a fatal threat to the personal and property safety of users, and even cause a major information security accident to the whole society. Based on a post-quantum cryptography system, this paper proposes a practical privacy protection scheme for ride-hailing route information, which can present the complete statistical aggregation operation of the route and the frequency from the starting point to the destination without the visibility of the ride-hailing platform, and ensure the data privacy security of a single vehicle. Compared with representative multi-vehicle aggregation solutions, we not only guarantee message privacy, confidentiality, integrity, forward and backward security, anti-man in attack and anti-redial attack, but also achieve multi-dimensional aggregation, CCA security and anti-quantum attack. Through the analysis of the experiment, the cost of our scheme is reasonable. Therefore, the scheme is more practical in this scenario.

INDEX TERMS Internet of vehicles, privacy protect, post quantum, data aggregation.

I. INTRODUCTION

The Internet of Vehicles (IoV) is derived from the Internet of Things, which is the Internet of things for vehicles. With the help of the new generation of information and communication technology, it realizes the network connection between cars and people, cars, roads and cloud platforms, so as to improve the overall intelligent driving level of the vehicle, and provide users with safe, comfortable, intelligent and efficient driving experience and traffic service. Also, it improves the efficiency of traffic operation and enhances the intelligence level of social traffic service. Meanwhile, thanks to the recent explosive growth of the ride-hailing business, a large amount of private information is collected through the IoV, which includes user starting point information, vehicle conversation information and vehicle driving record, etc. This information will help build a more efficient and intelligent solution to the IoV, which will make a significant contribution to improving the user experience and alleviating road traffic congestion.

However, this mass collection of information raises wide concern. It is feared that once the information of IoV is exposed by the online ride-hailing platform or stolen by hackers, this will pose a fatal threat to the personal and property safety of users, and even cause the whole society a major information security accident. Therefore, the security of privacy becomes particularly important. It is necessary to build a multi-party data and information trust mechanism for users, platforms and government agencies.

To do this, there are many privacy security challenges to address [16]. These include how to establish identity trust networks between vehicles, between vehicles and base stations, and between base stations and control centers; how to prevent hackers from attacking the network system in coalition with other members of the Internet of vehicles, eavesdropping or tampering with the message, setting up pseudo base stations to intercept the sender’s message and return the query information, etc.

Attempts have been made to tackle these challenges. Liu et al., Song et al., Li et al., He et al., Xue et al., and Saleem et al. [7]–[12] respectively proposed some simple sensing devices, privacy protection data collection and aggregation solutions for mobile devices, vehicle-mounted devices, smart grid and other application scenarios. These schemes can realize dynamic addition and deletion of members and...
allocation of calculations to each device, but they cannot meet other security requirements such as anti-quantum computing and anti-selective ciphertext attacks. In addition, there is the problem known as “the superior knows too much”. This is to say, operators may sell a large number of users’ personal information and behavioral privacy data, resulting in serious problems such as user behavior information leakage. For example, hackers can know when the user went from where to where, and how many times. To this end, we need to complete the aggregation of privacy protection data by integrating some of the technologies of previous solutions, and building trust between government and control centers, base stations and vehicles.

Then there is the issue of overhead. High overhead of the traditional communication network is fatal to the IoV scenario that relies on wireless sensing and micro-base station devices with weak computing power. Therefore, we need to adopt a third-party trusted institution with certain authority to reduce the overhead.

There are several schemes we look at when developing our own. Qian et al. [1], [2] proposed three lightweight and quantum-resistant vector space-based privacy protection data aggregation schemes on smart grid, which can aggregate multidimensional data. Based on this scheme, Lin and Qian [3] proposed a post-quantum SAAS platform, which can also achieve secure financial statistics. Based on this, this paper proposes a more practical scheme, which can aggregate multiple departure points, corresponding destinations and corresponding times simultaneously within a valid period. In addition, we have the following innovations compared with the representative multiple internet-of-vehicles aggregation solutions:

1. Our scheme not only realizes message privacy, confidentiality, integrity, forward and backward security, anti-man in attack and redial attack, but also realizes multidimensional aggregation, CCA security and anti-quantum attack.

2. Under our scheme, CC only knows how many times TA travels from the origin A to the destination B in a certain period of time without recording the details of authorization. But it does not know the total number of times TA travels, nor does it know the actual locations of A and B.

In addition, after TA authorization, the specific locations of A and B corresponding to the road sections with relatively large values can be decrypted. Therefore, so long as the specific time from A to B is protected, the frequency of the e-hailing vehicles passing through road sections can be known, thus bringing convenience to users and realizing more detailed data management and control.

The structure of this paper is as follows: Section 2 introduces PRELIMINARIES. Chapter 3 introduces the SYSTEM AND SECURITY MODEL. Chapter 4 introduces OUR PROPOSED SCHEME. Chapter 5 introduces the security analysis and proof of the scheme. Chapter 6 shows that we have low overhead through experiments. The last chapter is the summary of the whole paper.

II. GUIDELINES FOR MANUSCRIPT PREPARATION
A. RSA-OAEP CRYPTOGRAPHY
RSA [13] algorithm is one of the most commonly used public key encryption algorithms. Because of its homomorphism, CCA cannot be protected against selected ciphertext attacks. The RSA-oaep [14] obtained by adding salt to RSA can achieve CCA security, as it reduces the difficult problem to a one-way limited gate function.

B. LATTICE-BASED HOMOMORPHIC ENCRYPTION ALGORITHM BASED ON HLP PROBLEM
Firstly, we introduce the Hidden Lattice Problem (HLP). HLP is defined by Aguilar-Melchor and Gaborit [5]. Wieschebrink demonstrated in [6] that it is NP-complete and resistant to quantum computing. Then, in Melchor et al. [4], [5], two lattice homomorphic encryption schemes are given. Qian et al. [1] modified some flawed formulas, correctness verification process and security proof of these algorithms to make them correct and secure, and applied them in the field of smart grid to put forward a very lightweight privacy protection data aggregation scheme. The process of the algorithm is shown in Table 1 (All symbols in the scheme are completely consistent with [1], where the number of homomorphic operations can be regarded as sufficiently large):

| TABLE 1. Lattice cryptosystem based on HLP. |
|---------------------------------------------|
| **ENCRYPTION** | **DECRYPTION** |
| Input/Output: a message \( m \in \mathbb{Z}_p^N \) \( a \) ciphertext \( c \in \mathbb{Z}_p^{2N} \). | Input/Output: a ciphertext \( c \in \mathbb{Z}_p^{2N} \) / a message \( m \in \mathbb{Z}_p^N \). |
| 1: For each \( i \in \{1,2,...,n\} \) contrast randomly the disturbing vectors \( r_i \in \mathbb{Z}_p^N \). | 1: The receiver computes \( \varepsilon = (c_D - c_U A^{-1}B)A^{-1} \) \( \Delta^{-1} \) |
| 2: \( c = m \ast M_0 + \sum_{i=1}^{n} r_i \ast M_1 \) \( (1) \) | 2: \( c_D \) and \( c_U \) are the undisturbed and disturbed halves of \( PS^{-1}(c) \), and \( \varepsilon = (\varepsilon_1,\varepsilon_2,...,\varepsilon_N) \) \( (2) \). |
| **ENCRYPTION** | **DECRYPTION** |
| 2: \( c = m \ast M_0 + \sum_{i=1}^{n} r_i \ast M_1 \) \( (1) \) | 2: For each \( j \in \{1,2,...,N\} \), |
| 3: For any \( 1 \leq j \leq N \), if \( e_j \mod q > p - q / 2 \), \( \varepsilon_j = e_j \mod p - p \) \( (4) \); | then, if \( e_j \mod q < q / 2 \), \( u_j = \varepsilon_j \mod q \) \( (5) \); |
| else \( u_j = e_j \mod q - q \) \( (6) \) and \( m_j = (e_j - u_j) / q \) \( (7) \); | 3: For any \( 1 \leq j \leq N \), if \( m_j \geq r \), carry bits until \( 0 < m_j < r \). |
| Output \( m = (m_1,m_2,...,m_N) \) \( (8) \). | Output \( m = (m_1,m_2,...,m_N) \) \( (8) \). |

III. SYMBOL, SYSTEM MODEL AND SECURITY MODEL
A. SYMBOL
All symbols used in the system model and scheme in this paper are shown in Table 2.
TABLE 2. Lattice cryptosystem based on HLP.

| Parameter symbol | Meaning                                      |
|------------------|----------------------------------------------|
| CC               | Control Central                              |
| BS               | Base Station                                 |
| TA               | Trusted Authority                            |
| Car              | Smart Car                                    |
| ID               | Identity                                     |
| rID              | The privacy random number of the car with the ID |
| T                | The time stamp of each participant           |
| nBS              | The number of BS                             |
| nCAR             | The number of CARs in each BS                |
| TMessage         | Average number of messages sent by each CAR to BS during a period of time |
| StarID,i         | The starting coordinates of the car numbered as ID on the $i^{th}$ run |
| Endm,i           | The ending coordinates of the car numbered as ID on the $i^{th}$ run |
| TID,i, Star, End | The start and finish time of the $i^{th}$ run of the car with ID |
| Num ID, Start, End | The number of times a car ID goes from Start to End |
| Dis ID, Start, End | Total distance of miles traveled by cars with ID |
| T[i,i]           | the $i^{th}$ journey time interval of the car numbered with ID |
| s                | Current message upload time                  |
| N                | The vector dimension of a cipher (lattice-based) |
| K                | Security parameter                           |
| h(.)             | Hash function: $\{0,1\}^k \rightarrow \{0,1\}^{256t}$ ($t$ is the number of message blocks) |
| Enc(.)           | Use the encryption part based on the RSA-OAEP cryptosystem |
| Dec(.)           | Use the decryption part based on RSA-OAEP cryptosystem |
| p, q             | Two primes in RSA-OAEP                       |
| Q                | Module $p \times q$ in RSA-OAEP              |
| e                | Public key in RSA-OAEP                       |
| skBS-CC          | The shared key between BS and CC             |
| skCAR-BS         | The shared key between CAR and BS            |
| tID              | Random number                                |

**B. SYSTEM MODEL**

Fig. 1 shows that the network system structure model in this paper is composed of a government Trusted Authority (TA), semi-honest Control Center (CC), multiple Base Stations (BS) and multiple Cars (CAR) through a lightweight wireless network connection. Each CC connects to multiple BSs and each BS connects to multiple CARs. The following describes the functions and permissions of each section:

1. The TA takes charge of the primary key and authorizes CC to decrypt the message under the corresponding permission.
2. CC holds part of the key and can view part of the information authorized by TA. For example, from a partially authorized place to a place how many times the total number of cars passed, the total distance traveled by each car. For the rest of the information, CC can only get ciphertext such as user information and total driving distance and has no permission to decrypt it.
3. Each BS has its own secret real ID information and the corresponding hash value $h(ID)$, which is stored in a secure register along with other data. Only $h(h(ID) + rID)$ is disclosed to the public. BS also needs to count and encrypt the number of times each vehicle has traveled between the starting point and the destination point over a period of time.
4. Each CAR has its own private real ID information and the corresponding hash value $H(ID)$ and the private random number $r_{ID}$, and stores it in a secure register with other data. Only $h(h(ID) + r_{ID})$ is open to the public, and the coordinates of the start and destination of each drive, as well as the corresponding timeline, also need to be encrypted. In addition, the distance traveled over a period of time also needs to be encrypted.

**C. SECURITY MODEL**

Assume that CC, BS and Car are semi-honest (cannot submit fake data during aggregation but can maliciously attack others). Based on the international security and privacy requirements of cloud Internet of Things [15], we built our security model, including the following parts:

- Anti-middleman attack replay attack target
  - If opponent A takes a middleman attack or replay attack, it cannot get any valid information.
- Public key part CCA security target
As for the public key part of the scheme, the adversary A cannot obtain any valid information by using the selected ciphertext attack.
- Structural safety objective
The adversary A cannot obtain valid information by intercepting the message and enumerating it in combination with the member’s public parameters.
- Privacy, message authenticity, integrity, and confidentiality goals
Adversary A cannot extract any useful information from the intercepted messages, nor can it forge its real identity to participate in the aggregation process. And when it tries to modify the message, the malicious behavior will be detected.
- Back and forth to the safety target
When the shared key is leaked, the data security of the previous and next time is not affected.

IV. OUR PROPOSED SCHEME
A. INITIALIZATION PHASE
1. Each CAR generates its own public and private key pair for receiving data using the 2048-bit RSA-OAEP algorithm and exposes its own public key.
2. Firstly, TA generates its own 1024-bit public key encryption function Enc_TA(·) based on RSA-OAEP, and then the hash function h IDs are distributed to all participating members and recorded h(ID), the IDS of BS and CAR are denoted as ID_BS and ID, respectively, and the corresponding hash values are h(ID_BS) and h(ID_i) in addition. They were given random numbers r_BS and r_ID_i, which were held synchronously by TA. While CC and BS only have h(ID_BS) + r_BS and h(ID_i) + r_ID_i respectively, and they promulgate their ID values as h(h(ID_BS)) and h(h(ID_i)).
3. TA generates a large database, and the start and end points are arranged in order. In addition, Enc_TA(·) is used to encrypt the location, and CC and BS are stored synchronously in order to reduce their burden.
4. TA issues a random aggregated number R_BS to each BS and tells CC the total value of \( \sum R_BS \).

B. AGGREGATION PHASE
1. The honest and curious CAR (Its ID is ID_i and its name is recorded as CAR_ID) takes the three parts (starting point Star_ID,j and its time, the end point End_ID,j and its time as well as the precise identification signature with the sending time). The messages are encrypted with TA’s public key and then signed with its own RSA-oaep private key respectively to get Dec_CAR \( \left( \text{Enc}_TA\left( \text{Star}_{ID,j}, \text{End}_{ID,j}\right), T_{ID,j} \right) \). After the shared key on XOR, The message will be sent to BS by CAR within 5s to ensure the validity of time T.
2. After receiving the message, BS first decrypts the message with the shared key on XOR, and then uses the public key Enc_CAR, (·) and the identity signature h(h(ID_i) + r_ID_i + T) to verify the authenticity of the data. If the authentication fails, a message is sent by BS and the message is retransmitted by CAR (the transmission process of the short message is less than 45s to ensure that the identity can pass the authentication normally).
3. After the verification is successful, BS first records and stores some information from the car numbered h(ID_i) + r_ID_i, for example, the 4th path and time period of \( \text{Enc}_TA\left( \text{Star}_{ID,j}, \text{End}_{ID,j}\right), T_{ID,j} \), and add the number of trips Num_i(h(ID_i)+r_ID_i, Enc_TA(Star_ID,j), End_ID,j)) on the corresponding section of the route by 1.

Note, the correctness of the scheme is easy to verify, so no further details are needed.
C. QUERY PHASE

If CC wants to know the elapsed time between Start and End, there is no way to directly encrypt with TA’s public key and then compare it with the database (because the algorithm is salt-added, the data cannot be matched without decrypting). Therefore, it must be encrypted first and then sent to TA. TA decrypts and matches the data before encrypting the serial number and sending it to CC. CC will know how many times a period of time he wants to know.

D. DYNAMIC MEMBERSHIP PHASE

On the one hand, you can see from the initialization process, in the network, adding a CAR and deleting a CAR have little overhead.

On the other hand, adding a BS and assigning it a new random number $R_{\text{new}}$, through its public key, and the random number before the update is $R: = R + R_{\text{new}}$, so the dynamic flexibility of the number is valid.

V. SECURITY ANALYSIS AND PROOF

This section mainly introduces the security analysis and proof of the solution, which is divided into the following parts:

**Theorem 1:** (Structure Security Theorem) Plaintext $t$ (or $t'$) in $M$ and ciphertext $s$ (or $s'$) in $C$ are adversary $A$ breached the advantage of any one node function $\text{Adv}_{t,A,M,C} = \max\{|\text{Pr}[t = t'] - \frac{1}{2}|, |\text{Pr}[s = s'] - \frac{1}{2}|\}$ is negligible.

**Proof:** According to Qian et al. [1], it can be known that if we want to achieve post quantum security, the advantage of indistinguishable function must be exponentially negligible. So according to the derivation, we have

$$\text{Adv}_{t,A,M,C} = \max\{|\text{Pr}[t = t'] - \frac{1}{2}|, |\text{Pr}[s = s'] - \frac{1}{2}|\} = \max\left\{\frac{1}{r^N}, \frac{1}{C^N}\right\} = \max\left\{\frac{1}{r^N}, \frac{2N + 1}{2^{2N}}\right\} < \varepsilon.$$

Structure Security is always true, so the system is safe.

**Theorem 2:** (Privacy, Message Authenticity, Integrity, and Confidentiality Theorems) Adversary $A$ cannot destroy the privacy of the scheme, tamper with message authenticity, destroy data integrity, and steal confidentiality.

**Proof:** First of all, according to the **Theorem 1** and the shared key, the message obtained by adversary $A$ is encrypted with the shared key and random numbers, so privacy can be guaranteed according to this. In the process from CAR to BS, if the message in the round is obtained, since $h(h(I_{Di}) + r_{Di} + T)$ has used timestamp and ID after the private key signature, the sender’s ID must be real and the message must be complete, otherwise the authentication cannot be passed. Therefore, the authenticity and integrity of the message are guaranteed. In the process from BS to CC, if the message in this round is obtained, because after the private key is signed,

$$h(h(I_{BS}) + r_{BS} + T, CNum') || CNum'$$

along with a timestamp and ID and message of the signature, the identity of the message sender must be truthful and message must be complete, otherwise cannot be verified. The adversary $A$ cannot get CC’s private key and shared key, so it can’t forge CC and can’t destroy the privacy, integrity and confidentiality of CC’s message. CC and TA are directly point-to-point secure channel authentication; hence they can also do the above properties.

**Theorem 3:** Adversary $A$ is unable to perform a replay attack and a middleman attack on this program.

**Proof:** Because of the automatic timestamp mechanism, the ID is dynamic, and opponent $A$ cannot launch a replay attack on our scheme. In addition, because the signature cannot be verified even if the identity is leaked, enemy $A$ cannot act as a middleman to some extent.

Sincerely, since the Adversary has a dynamic key of some round, it breaches the advantage of any one node function

$$\text{Adv}_{t,A} = \max\{|\text{Pr}[key = key] - \frac{1}{2}|\} < \varepsilon.$$

This scheme can achieve a replay attack and a middleman attack on this program.

**Theorem 4:** This scheme satisfies the differential privacy nature.

**Proof:** The scheme adopts salt-added RSA signature and lattice-homomorphic cryptosystem to satisfy the differential privacy. Therefore, the condition $\text{Adv}_{t,A,M} < \varepsilon$ is satisfied in terms of public key cryptosystem. From the perspective ofplaintext message collision,

$$\text{Adv}_{t,A,M} = \max\{|\text{Pr}[t = t'] - \frac{1}{2}|\} = \max\left\{\frac{1}{r^N}\right\} < \varepsilon.$$

Hence, this scheme satisfies the differential privacy nature.

**Theorem 5:** (Forward and Backward Security Theorem) When the key is leaked, the data security of the previous and next time will not be affected.

**Proof:** It assumes that the difficulty of cracking the shared key is $\varepsilon$. Since the Adversary has a secret shared key of some round, it breaches the advantage of any one node function

$$\text{Adv}_{t,A} = \max\{|\text{Pr}[key = key] - \frac{1}{2}|\} < \varepsilon.$$

This scheme can achieve forward and backward security.

**Theorem 6:** (CCA Security Theorem) Our scheme can resist select ciphertext (geographic location information, etc) attack in the public key part, so the security reaches CCA security level.

**Proof:**

$$\text{Dec}_{CAR}(\text{Enc}_{TA}(\text{Star}_{Di}, i, \text{End}_{Di}, j), \text{T}id_{Di,j})$$

The security of the public key part of the scheme depends on the security of the RSA-OAEP cryptography scheme, which can reach the CCA security level [10], as the result, the public key part of our scheme can reach the CCA security level.

**Theorem 7:** This scheme can resist differential privacy to some extent.
Proof: The opponent will not obtain a valid random number \( r \) from the value of \( m + r \) when the message \( m = 0 \).

In addition, we compared the security of previous schemes with our own and obtained the results as shown in Table 3 (Indicators are Post Quantum Attack(P1), Privacy, Entity Authentication and Authenticity of message(P2), Forward Backward Security(P3), Differential Privacy(P4), Anti Man in the Middle(P5), Replay Attack(P6), Flexibility of Network Structure(P7)). Therefore, our scheme has more comprehensive security.

| TABLE 3. Parameter symbol and meaning. |
|--------------------------------------|
| Scheme | P1 | P2 | P3 | P4 | P5 | P6 | P7 |
|--------|----|----|----|----|----|----|----|
| [7]    | N  | Y  | N  | N  | N  | N  | N  |
| [8]    | N  | Y  | N  | N  | N  | N  | N  |
| [9]    | N  | Y  | N  | N  | N  | N  | N  |
| [10]   | N  | Y  | N  | N  | N  | N  | N  |
| [11]   | N  | Y  | N  | N  | N  | Y  |   |
| [12]   | N  | Y  | N  | Y  | N  | Y  | Y  |
| Ours   | Y  | Y  | Y  | Y  | Y  | Y  | Y  |

VI. PERFORMANCE EVALUATION
This section provides an analysis of the communication and computational costs of our proposed scheme. We implemented our solution using a Python 3.7 environment on a computer with a 3.00ghz processor, 4GB of RAM, and Intel Core-i5CPU. See Table 4 for parameter settings.

| TABLE 4. Parameter value. |
|---------------------------|
| Parameter                | Value                       |
| Parameters based on HLP lattice cipher | It is consistent with reference [1] |
| \( n_{\text{BS}} \)       | 1-10                        |
| \( n_{\text{CAR}} \)      | 1-100                       |
| Total number of paths    | 1000                        |
| \( n_{\text{Message}} \)  | 20-50                       |

Then, the communication and computational overhead of the aggregation process is analyzed theoretically.

A. COMMUNICATION OVERHEAD
The message sent by CAR to BS is

\[
\text{Dec}_{\text{CAR}} \left( \text{Enc}_{\text{TA}} \left( \text{Star}_{\text{ID}}, \text{End}_{\text{ID}}, T_{\text{ID}} \right), T_{\text{ID}} \right)
\]

The length of the message is 2048 bits. Therefore, the total size of the message received by all BS is about 2048 \( \times n_{\text{Message}} \times n_{\text{CAR}} \times n_{\text{BS}} \) bits. The total size of message

\[
h \left( h \left( ID_{\text{BS}} \right) + r_{\text{BS}} + T, C_{\text{Num}} \right) || C_{\text{Num}}'
\]

sent by BS to CC is about 1200 \( \times (z + 1) \times n_{\text{BS}} \) bits, where \( z = 2 \). So the total communication overhead is approximately

\[
(2 \times n_{\text{Message}} \times n_{\text{CAR}} \times n_{\text{BS}} + 3 \times n_{\text{BS}}) kb 
\]

\[
\ll (100030) kb \ll 100Mb
\]

Therefore, the communication overhead is acceptable.

B. COMPUTATION OVERHEAD
\( t_{\text{HLP-ENC}} \) and \( t_{\text{HLP-DEC}} \) respectively represent the time of one round of encryption and decryption using HLP lattice password; \( t_{\text{RSA-ENC}} \) and \( t_{\text{RSA-DEC}} \) respectively represent the time of one round of encryption and decryption using the public and private keys of TA; \( t_{\text{CAR-ENC}} \) and \( t_{\text{CAR-DEC}} \) respectively represent the average time for a round of signing and verification using the CAR public and private keys. \( t_{\text{hash}} \) indicates the average time for a round of signatures. Other simple addition operations cost much less than those above, so this can be ignored. Hence the total computational cost of the aggregation process is approximately

\[
( (t_{\text{RSA-ENC}} + t_{\text{RSA-DEC}} + t_{\text{CAR-ENC}} + t_{\text{hash}}) \times n_{\text{Message}} \times n_{\text{CAR}} + t_{\text{HLP-ENC}} + t_{\text{HLP-DEC}} ) \times n_{\text{BS}} \times \text{HLP-DEC}
\]

Then, the parallelization computation overhead time is

\[
( (t_{\text{RSA-ENC}} + t_{\text{RSA-DEC}} + (t_{\text{CAR-ENC}} + t_{\text{hash}}) \times n_{\text{CAR}} ) \times n_{\text{Message}} + t_{\text{HLP-ENC}} + t_{\text{hash}} + t_{\text{HLP-DEC}} ).
\]

Since the theoretical analysis is not obvious, we obtained the relationship between the total overhead, as shown in

FIGURE 2. \( n_{\text{Message}} \) and \( n_{\text{BS}} \).

Through the experimental calculation, we know that under the premise of \( n_{\text{BS}} = 10 \), \( n_{\text{Message}} = 50 \), the total computation cost is about 3175s, and the computation time after parallelization is about 53s, which is an extremely short and acceptable parallel computation time.

VII. CONCLUSION
Based on a post-quantum cryptography system, this paper proposes a practical privacy protection scheme for ride-hailing route information, which can make the statistical aggregation operation of the route and frequency from the starting point to the destination complete without the visibility of the ride-hailing platform, and ensure the data privacy
security of a single vehicle. Compared with representative multi-vehicle aggregation solutions, we not only achieve message privacy, confidentiality, integrity, forward and backward security, anti-man in attack and redial attack, but also achieve multi-dimensional aggregation, CCA security and anti-quantum attack. In addition, through the analysis of the experiment, the cost of our scheme is reasonable, thus, the scheme is practical in this scenario.

REFERENCES

[1] J. Qian, Z. Cao, X. Dong, J. Shen, Z. Liu, and Y. Ye, “Two secure and efficient lightweight data aggregation schemes for smart grid,” IEEE Trans. Smart Grid, vol. 12, no. 3, pp. 2625–2637, May 2021.
[2] J. Qian, Z. Cao, M. Lu, X. Chen, J. Shen, and J. Liu, “The secure lattice-based data aggregation scheme in residential networks for smart grid,” IEEE Internet Things J., vol. 9, no. 3, pp. 2153–2164, Feb. 2022.
[3] J. Lin and J. Qian, “A multi-party secure SaaS cloud accounting platform based on lattice-based homomorphic encryption system,” in Proc. Int. Conf. Public Manage. Intell. Syst.(PMIS), Feb. 2021, pp. 1–4.
[4] C. A. Melchor, G. Castagnos, and P. Gaborit, “Lattice-based homomorphic encryption of vector spaces,” in Proc. IEEE Int. Symp. Inf. Theory, Jul. 2008, pp. 1858–1862.
[5] C. Aguilar-Melchor and P. Gaborit, “A lattice-based computationally-efficient private information retrieval protocol,” in Proc. Western Eur. Workshop Res. Cryptol., 2007, pp. 337–343.
[6] C. Wieschebrink, “Two NP-complete problems in coding theory with an application in code based cryptography,” in Proc. IEEE Int. Symp. Inf. Theory, Jul. 2006, pp. 1733–1737.
[7] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, “A practical privacy-preserving data aggregation (3PDA) scheme for smart grid,” IEEE Trans. Ind. Informat., vol. 15, no. 3, pp. 1767–1774, Mar. 2019.
[8] J. Song, Y. Liu, J. Shao, and C. Tang, “A dynamic membership data aggregation (DMDA) protocol for smart grid,” IEEE Syst. J., vol. 14, no. 1, pp. 900–908, Mar. 2020.
[9] X. Li, J. Li, S. Yiu, C. Gao, and J. Xiong, “Privacy-preserving edge-assisted image retrieval and classification in IoT,” Frontiers Comput. Sci., vol. 13, no. 5, pp. 1136–1147, Oct. 2019.
[10] W. He, H. Nguyen, X. Liuy, K. Nahrstedt, and T. Abdelzaher, “IPDA: An integrity-protecting private data aggregation scheme for wireless sensor networks,” in Proc. IEEE Mil. Commun. Conf., Nov. 2008, pp. 1–7.
[11] K. Xue, B. Zhu, Q. Yang, D. S. L. Wei, and M. Guizani, “An efficient and robust data aggregation scheme without a trusted authority for smart grid,” IEEE Internet Things J., vol. 7, no. 3, pp. 1949–1959, Mar. 2020.
[12] A. Saleem, A. Khan, S. U. R. Malik, H. Pervaz, H. Malik, M. Alam, and A. Jindal, “FESDA: Fog-enabled secure data aggregation in smart grid IoT network,” IEEE Internet Things J., vol. 7, no. 7, pp. 6132–6142, Jul. 2020.
[13] P. Barrett, “Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor,” in Proc. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 1986, pp. 311–323.
[14] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern, “RSA-OAEP is secure under the RSA assumption,” in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2004, pp. 260–274.
[15] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and privacy for cloud-based IoT: Challenges,” IEEE Commun. Mag., vol. 55, no. 1, pp. 26–33, Jan. 2017.
[16] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, “Security challenges in vehicular cloud computing,” IEEE Trans. Intell. Transp. Syst., vol. 14, no. 1, pp. 284–294, Mar. 2013.

CHENG WEI received the bachelor’s degree in software engineering from the Jiangxi University of Finance and Economics and the master’s degree in computer science from the School of Software, Huazhong University of Science and Technology, in 2019. His current research interests include cryptography and artificial intelligence algorithms.

TAO WU received the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, China, in 2002, where he is currently a Professor with the School of Software. His research interests include computer information and artificial intelligence.

XINGYU LIU, born in Jingzhou, Hubei, in 1998. He received the graduate degree from the School of Mechanical and Electrical Engineering, Wuhan University of Technology. He is currently pursuing the master’s degree with the School of Cyberspace Security, Huazhong University of Science and Technology. His main research interest includes optimization algorithms.

SHUO XIONG received the master’s and Ph.D. degrees in information science from the Advanced Institute of Science and Technology, Japan. He is an Assistant Professor with the School of Journalism and Information Communication, Huazhong University of Science and Technology. His research interests include game informatics, game theory and AI, serious game, and game design.