Abstract
In the process of crowdsensing, tasks allocation is an important part of the precise as well as the quality of feedback results. However, during this process, the applicants, the publisher and the authorized agency may be aware of the location of each other, and then threaten their privacy. Thus, in order to cope with the problem of privacy violation during the process of tasks allocation, in this paper, based on the basic idea of homomorphic encryption, an encrypted grids matching scheme is proposed (short for EGMS) to provide privacy preservation service for each entity that participates in the process of crowdsensing. In this scheme, the grids used for tasks allocation are encrypted firstly, so the process of task matching by applicants and publishers is also in an encrypted environment. Next, locations used for allocation as well as locations that applicants can provide services are secrets for each other, so that the location privacy of applicants and publishers can be preserved. Finally, applicants of task feedback results of each grid that they located in, and the publisher gets these results, and the whole process of crowdsensing is finished. In the last part of this paper, four types of security analysis are given to prove the security between applicants and the publisher. Then several groups of experimental verification that simulates the task allocation are used to test the security and efficiency of EGMS, and the results are compared with other similar schemes, so as to further demonstrate the superiority of our proposed scheme.

Keywords Crowdsensing · Homomorphic encryption · Location privacy · Privacy preservation · Tasks allocation

Xiaodong Zheng
Inxiaodong@163.com

1 College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, People’s Republic of China
2 College of Computer Control and Engineering, Qiqihar University, Qiqihar 161006, People’s Republic of China
3 College of Communication and Electronic Engineering, Qiqihar University, Qiqihar 161006, People’s Republic of China
4 College of Information Science and Electronic Technology, Jiamusi University, Jiamusi 154007, People’s Republic of China
1 Introduction

Recently, with the prosperous development of wireless communication as well as the application of 5G wireless system, mobile devices such as smartphones and tablet computers are widely used in nearly all aspects of people’s daily life [1–3]. Then devices that equipped plenty of sensing modules (such as GPS, the temperature sensor, the gyroscope and so on) can be used to gather sensing information in vicinity, and the collected information can be sent to the research department or government to further improve the quality of people’s daily life [4–6]. In general, the process of collecting sensing information from applicants is termed crowdsensing and the definition of crowdsensing mainly refers to the method of obtaining sensing information from the distribution of mobile devices [7, 8]. During the process of crowdsensing, the publisher does not need to arrive at the sensing place and can get the update sensing information in real time, and the applicant can obtain a certain number of rewards from the publisher. As a result, both the publisher and the applicant will benefit from each other, as the publisher will get the sensing information with a lower expenditure on information collection and the applicant will get an incentive with just a bit of sensing information transformation [9–11].

However, along with the convenience of this type of service, the risk of privacy violence cannot be neglected [12–14]. For example, if a publisher wants to get the temperature variation of a specific region, he will send the sensing request to the authorized agency or broadcast the sensing request to all potential applicants. Then applicants that are located in this region will feed back the sensing result to the publisher and get rewards from the publisher. During the process of publishing the request and getting feedback results from applicants, the publisher will learn the location of the applicant and the applicant will be aware of the sensing location of the publisher. In addition, these locations will also be released to the authorized agency. If an entity in the crowdsensing is un-trusted, the personal privacy of the publisher or the applicant will be violated [15, 16]. Thus, in order to cope with the problem of privacy violation in the process of crowdsensing, Yang et al. [17] utilized the model of differential privacy to deal with the density of sensing applicants and generated a location privacy preservation scheme for mobile crowdsensing. But this scheme mainly depends on adding dummies to generalize the real location, which will bring the lack of accuracy for feedback result. Thereafter, in order to cope with the same problem, Yang et al. [18] utilized the conception of distributed consensus from the blockchain to achieve the location privacy preservation of task allocation in crowdsensing. But the collaboration of this scheme will be affected by the willingness of collaborative users in the public chain. Then, in recent years, along with the deepening research of crowdsensing, more schemes for preserving personal privacy are proposed. For example, the scheme of privacy preservation bus sharing [19], the scheme of sparse region sensing [20], the scheme for adjacent sensing [21] as well as the scheme for privacy recommending members [22] and so on.

Although schemes mentioned above can provide privacy preservation service for the publisher and the applicant in a certain extent, they do not achieve the closed loop of information transformation for entities in the crowdsensing, i.e. these schemes usually assume that the authorized agency is a trusted entity (such as the scheme of privacy preservation bus sharing [19] and the scheme of sparse region sensing [20]) or mainly designed for preserving the privacy of applicants (such as the scheme for adjacent sensing [21] and the scheme for privacy recommending members [22]). In addition, schemes used recently usually neglect that the publisher also needs to preserve the personal privacy of his own. Thus, in order to cope with the violation of location privacy in the process of task allocation in
crowdsensing and ensure during the process of task allocation no information about each entity can be released to any entity. In this paper, based on the conception of homomorphic encryption and encrypted grids matching, a privacy preservation scheme for the task allocation in crowdsensing has been proposed based on Paillier encryption system. In this scheme, we mainly focus on the security problem of task allocation, and provide privacy preservation service for both the publisher and applicants simultaneously. With the Paillier encryption system, the process of tasks matching is encrypted, and no entity can get the precise location of each other. Then the publisher decrypts the result of matching and decides whether to launch another round of tasks allocation. As a result, this scheme will increase the security of crowdsensing and improve the user experience, and then further enhance the development of this application in the industry.

The contribution of this paper can be summarized as the follows.

(1) A privacy preservation scheme for the task allocation in crowdsensing has been proposed. With this scheme, the personal location privacy for both the publisher and the applicant is preserved and even the authorized agency also difficult to get any privacy about them.

(2) We give a formal definition of EGMS and also give several groups of formal analysis to justify the security and feasibility of our proposed scheme.

(3) An experimentally compare and evaluate is given to verify the performance of the proposed scheme, and the result with brief instruction has further demonstrates the superiority of EGMS.

According to the contribution, we organize the remainder of this paper as the follows. In Sect. 1, we present the system architecture and definitions. Section 2 presents our proposed EGMS, and then we discuss three algorithms and develop the details. In Sect. 3, based on the theoretic analysis, we discuss the security and feasibility of EGMS. In Sect. 4, we give the simulation model and discuss the simulation results. Finally, we give more related work related with EGMS in Sect. 5, and conclude our work and discuss further work in Sect. 6.

2 The System Architecture and Definitions

2.1 The System Architecture

In general, a basic process of task allocation for crowdsensing can be conducted by three entities, and these entities can be called the publisher, applicants as well as the authorized agency. The publisher mainly refers to the user who wants to get crowdsensing results from others, and issues rewards as the incentive to a user who provides the precise result. The applicants refer to a group of users that send crowdsensing results to the publisher and obtain incentives. The authorized agency refers to an organization that is generated by the government or large enterprises, which can provide central services to publish crowdsensing tasks or incentive rewards. As shown in Fig. 1, in the process of crowdsensing, the publisher first sends the request of crowdsensing and the location grids of task allocation to the authorized agency. Next, the publisher publishes its public key to all applicants, so as to guarantee the security of feedback results. Once the authorized agency receives the request, this entity publishes the request to applicants. Then each applicant checks its location grid. If the grid matches request, this applicant sends the crowdsensing result to the authorized
agency. Otherwise, the applicant waits for other tasks. The authorized agency collects all crowdsensing results and generates a set of these results, and then sends this set to the publisher. At the same time, the authorized agency issues incentives to all applicants who have sent the precise crowdsensing result by their locations.

Based on the system architecture and the brief process of crowdsensing shown in Fig. 1, the location privacy of the publisher as well as the location privacy of the applicant will be violated in the step of tasks allocation and the step of results feeding back. In general, the location is a crucial condition that must be used to confirm where the crowdsensing task is needed, and where is the feeding back result the applicant can provide. With the precise location of the applicant, a malicious publisher can publish this information to others with commercial exploitation or push advertisement. With the precise location of the publisher, a malicious applicant can construct inaccurate feedback results and utilize it to obtain the incentive. Furthermore, when the authorized agency matches a task he can also get information about locations from both publisher and applicant, so the location awareness matching further jeopardizes location privacy of both parts of entities in crowdsensing. In conclusion, the privacy violation of crowdsensing system is a serious problem, and it is also a complicated issue for each entity to preserve its own location privacy. Thus, a scheme used in tasks allocation that can provide location privacy for three entities simultaneously and guarantees each entity cannot get the precise location is needed.

### 2.2 The Paillier Homomorphic Encryption

As in the process of crowdsensing, the publisher, applicants and the authorized agency may be aware the location of each other, and then threaten the privacy of them (as shown in Fig. 1), a scheme is needed to find the best solution to publish a task with confidential location matching. As a result, three entities in the process of task allocation cannot obtain any information about each other. For confidential calculation, the strategy of homomorphic encryption is a better idea, as the result of calculation with encrypted parameters is identical to the result of calculation without encryption. Thus, in this paper, Paillier’s public-key
cryptosystem is considered to be used in the process of confidential location matching, and the workflow of this cryptosystem can be described as follows.

Firstly, two different large prime numbers \( p \) and \( q \) are selected randomly, and these numbers satisfy \( \gcd(pq, (p - 1)(q - 1)) = 1 \). Then calculates \( N = pq \), and randomly selects a integer \( g \in \mathbb{Z}^*_N \), publishes the public key \( pk = (N, g) \), preserves the private key \( sk = (p, q) \).

The process of encryption: for the given public key \( pk \) and the plaintext \( m \) (which is an integer less than \( N \)). Then selects a random integer \( r \) from the set of \( \mathbb{Z}^*_N \), and calculates the ciphertext with \( c = g^m r^N \pmod{N^2} \). For two parts of the given plaintext \( m_1, m_2 \in \mathbb{Z}^*_N \), the encryption satisfies the following characters.

\[
E(m_1)E(m_2) = E(m_1 + m_2),
\]

\[
E(m_1)^{m_2} = E(m_1m_2).
\]

The process of decryption: for the ciphertext \( c \), \( \lambda \) is the lowest common multiple (LCM) of \( (p - 1) \) and \( (q - 1) \), where \( \lambda = \text{lcm}((p - 1), (q - 1)) \), and then the plaintext can be get with

\[
m = \frac{(c^\lambda \mod N^2 - 1)/N}{(g^\lambda \mod N^2 - 1)/N \mod N}.
\]

So based on characters of confidential addition method mentioned above, a confidential location matching scheme can be devised to solve the privacy problem in crowdsensing.

### 3 The Scheme of Encrypted Grids Matching

#### 3.1 The Basic Idea and Conception

In the process of crowdsensing tasks allocation, the region of sensing can be divided into square areas with multi-grids. Then the user who locates in the specified grid can be seen as an applicant, once he accepts the request of sensing task and can feed back sensing result for the publisher. So the applicant usually takes mobile sensing devices along with his moving and can communicate with the publisher and the authorized agency. In order to find plenty of applicants to satisfy the request of the publisher, the authorized agency also needed, and utilized to publish tasks and collect feeding back results.

Therefore, based on the process of task allocation as well as multiple grids of sensing region, the basic idea and conception of privacy preservation can be concluded as four steps. In the first step, the authorized agency sets the sensing region and grids, and the publisher and each applicant specifies the values of sensing and servicing grids with sensing request and sensing feedback ability. In the second step, the publisher and each applicant encrypts the grid values with the public key of Paillier encryption system, and both entities send the encrypted result to the authorized agency. In the third step, the authorized agency calculates the result of matrix matching by the encrypted values from the publisher and applicants and sends the matching result to the publisher. The publisher checks whether the result of matrix matching satisfies the sensing request. If so, the publisher requests the authorized agency to collect encrypted results of crowdsensing from applicants. Otherwise, the publisher asks the authorized agency to publish the task once again and checks the result of matrix matching one more time. In the fourth step, the authorized agency collects
feedback results from all applicants and sends the result set to the publisher, and then the whole process of crowdsensing is over. The process of task allocation can be depicted as shown in Fig. 2.

Based on the process of task allocation, the range of sensing region is released to both the publisher and applicants and divided into grids by the authorized agency. Suppose the request grid of the publisher can be denoted as $A$ and the whole grid of applicants can be denoted as $B$. Then based on the conception of Paillier’s public-key cryptosystem, we have

$$E(C) = E(A) \cdot E(B) = E\left(\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}\right) \cdot E\left(\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix}\right)$$

where the element of encryption in each matrix is $E(a_{ij}) = g^{c_{ij}rN} \mod N^2$, $1 \leq i, j \leq n$.

When the authorized agency finishes the grid matching and gets $E(C)$, he sends this result to the publisher, and then the publisher decrypts $E(C)$ and gets the plaintext with $c_{ij} = \frac{(E(C)_{ij}^{rN} \mod N^2 - 1)/N}{(g^r \mod N^2 - 1)/N} \mod N$. If the result satisfies the request of sensing, i.e. the elements that denote the sensing grids are zero in the matrix $C$, the publisher grids matching is finished. Otherwise, the publisher launches a new round of sensing requests.

During this process, location information that the authorized agency receives from the publisher and applicants is encrypted with the Paillier encryption system, so the authorized agency knows nothing about the sensing grids without the private key. The feedback result also encrypted with the public key of the publisher, so the authorized agency also knows nothing about the feeding back result. For the publisher, there is nothing about location information about applicants sent to him, as the process of sensing grids matching is just conducted by the authorized agency. For applicants, the authorized agency also conducts sensing grid matching, and nothing about the publisher is sent to any applicant. Thus, as a result, during the whole process of tasks allocation in crowdsensing, there is nothing about
the location of each entity that can be obtained by any entity and the location privacy of them is preserved.

3.2 The Process of Location Privacy Preservation Crowdsensing Tasks Allocation

Based on the basic idea of privacy preservation that mentioned in Sect. 2.1, in this paper the process of tasks allocation in crowdsensing can be converted to the problem of confidential matrix matching. Thus, the authorized agency needs to divide the area of crowdsensing into a region with multiple grids, and broadcasts the matrix of these grids to other entities such as the potential publisher and the potential applicants, and then these entities can leverage the matrix to finish the conduct of location matching.

For example, suppose a sensing region can be converted to a three-by-three matrix. In this matrix, elements that the publisher does not want to get results of crowdsensing from are denoted as random numbers from 1 to 9, and elements that need to be sensed are denoted as 0. Thus, in the process of tasks allocation, the publisher utilizes this matrix and the specified grids with random numbers to finish the location matching. Next, the publisher encrypts each element in the matrix with the generated public key of Paillier encryption system and also broadcasts this public key to all applicants. As shown in Eq. 4, an area the publisher needs to sense is converted to a matrix and denoted as $A$, and elements of this matrix the publisher does not want to get sensing results from are signed as random numbers from 1 to 9, others are signed as 0. Then the publisher leverages the public key to encrypt each element in the matrix of $A$ and gets the encrypted matrix of $E(A)$.

$$E(A) = E\left(\begin{bmatrix} 2 & 0 & 4 \\ 0 & 8 & 0 \\ 1 & 6 & 0 \end{bmatrix}\right) = \begin{bmatrix} E(2) & E(0) & E(4) \\ E(0) & E(8) & E(0) \\ E(1) & E(6) & E(0) \end{bmatrix}.$$

(4)

After generating the encrypted matrix, the publisher sends this matrix and the incentive together to the authorized agency. Then the authorized agency broadcasts the request of sensing region to all users located in each grid and waits for applicants sent from the user who is located in each grid and willing to participate in crowdsensing. For the user, if he wants to participate in crowdsensing, he has to check whether his location is on the grid that can provide feedback results. If so, the user converts to an applicant and constructs the encrypted matrix with the public key of Paillier encryption system as shown in Eq. 5. Otherwise, this user cannot be seen as an applicant and has to wait for another task. Like the process of the publisher, the applicant also denotes the elements in the grid matrix which he cannot provide crowdsensing results with random numbers from 1 to 9 and others are signed as 0. Then the applicant encrypts the elements in this matrix with the public key sent from the publisher, and gets the confidential matrix $E(B)$. Next, the applicant sends the encrypted matrix to the authorized agency.

$$E(B) = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} E(1) & E(2) & E(1) \\ E(0) & E(0) & E(0) \\ E(0) & E(0) & E(0) \end{bmatrix}.$$

(5)

Once various applicants apply for crowdsensing simultaneously, the authorized agency will receive several matrixes. Then the authorized agency constructs these matrixes into a matrix set and denotes it as $B_i, 0 \leq i \leq n$, (where $n$ is the
maximum of the publisher can reward these applicants), and then he calculates \( C = A \cdot B_1 + A \cdot B_2 + \cdots + A \cdot B_i \) and gets the encrypted result matrix without knowing anything about the value of each element. The encrypted result of calculation is then sent to the publisher and used to check whether it satisfies the request of the publisher. The process of calculation can be seen in Eq. 6. The matrixes of \( E(A) \) and \( E(B) \) that used in Eq. 6 are derived from Eqs. 4 and 5.

\[
E(C) = E(A) \cdot E(B) = \begin{bmatrix}
E(2+1) & E(0+2) & E(4+1) \\
E(0+0) & E(8+0) & E(0+0) \\
E(1+0) & E(6+0) & E(0+0)
\end{bmatrix} = \begin{bmatrix}
E(3) & E(2) & E(5) \\
E(0) & E(8) & E(0) \\
E(1) & E(6) & E(0)
\end{bmatrix} = E\left(\begin{bmatrix}
3 & 2 & 5 \\
0 & 8 & 0 \\
1 & 6 & 0
\end{bmatrix}\right).
\]

(6)

The publisher then decrypts the matrix \( C \) with the private key from Paillier encryption system. If the decrypt matrix contains all grids of the request, the publisher sends a message to the authorized agency to trigger the process of distributing incentives to the applicant who was concluded in this matrix set. Otherwise, the publisher sends a message to the authorized agency to initiate another request, and then the authorized agency releases the new request to the region which needs crowdsensing, so as to select other applicants.

In the condition of the matrix do not encrypted by Paillier encryption system, suppose the zero elements in the matrix \( A \) construct the grids need to be sensed, the zero elements in the matrix \( B \) denote the grid that this applicant can provide the result of crowdsensing. As a result, the zero elements in the matrix \( C \) which is calculated by \( A + B \) can be seen as the matched grids. Once the publisher collects enough grids with non-zero elements from various applicants, he will get all grids that he wants to obtain the sensing result as well as applicants in these grids, so that the task allocation of crowdsensing will be finished successfully.

### 3.3 The Process of Information Conduct (Tasks Publisher)

Suppose in matrix \( A \), elements that the publisher constructed for each grid can be denoted as \( a_{ij}, 0 \leq i, j \leq n \). Based on the Paillier encryption system, the encrypted element can be denoted as \( E(a_{ij}) \), which means the element is calculated by the public key of the publisher. Then the publisher sends the matrix with encrypted elements to the authorized agency. The process of establishing the confidential matrix for the publisher is shown in Algorithm 1.

**Algorithm 1**: The establishment of confidential matrix for the publisher  
**Input**: Location matrix \( A = a_{ij} \)  
**Output**: Encrypted location matrix \( E(A) = E(a_{ij}) \)

1. The publisher establishes a pair of public key and private key with Paillier algorithm;
2. For (\( j=0; j<=n; j++ \)) do
3. For (\( i=0; i<=n; i++ \)) do
4. \( E(a_{ij}) = g^{a_{ij}} \cdot r^N \) (\( \text{mod} \ N^2 \));
5. End For
6. End For
7. Return \( E(a_{ij}) \);
The process of getting public key from the Paillier encryption system has been mentioned in detail in Sect. 1.2, and in this paper we do not repeat it. In Algorithm 1, the confidential matrix of the publisher is constructed and denoted as \( E(A) \) which can be used to calculate the matching grids, and the element of this matrix is encrypted with the public key, so without the private key of the publisher, no one can infer the precise value of each element. Then this confidential matrix \( E(A) \) is sent to the authorized agency.

### 3.4 The Process of Information Conduct (Tasks Applicants)

Suppose that each applicant can get a public key \( pk = (N, g) \) from the broadcast by the publisher. Each applicant can establish a square region with the grids of providing sensing result, and then this region can be converted to a two-dimensional matrix denoted as \( B \), where the elements in this matrix correspond to the grids in this region and can be denoted as \( b_{ij}, 0 \leq i, j \leq n \). Then the applicant encrypts each element with the public key \( pk \) and gets the confidential matrix \( E(b_{ij}) \), and then submits this matrix to the authorized agency. In Algorithm 2 we show the process of how the applicant encrypts the matrix.

**Algorithm 2:** The establishment of confidential matrix for applicants

**Input:** The location matrix of applicants \( B = b_{ij} \)

**Output:** Encrypted location matrix \( E(B) = E(b_{ij}) \)

1. The applicant leverages the public key \( pk \) encrypts the location matrix of its own;
2. For (\( j = 0; j \leq n; j++ \)) do
3. \hspace{1em} For (\( i = 0; i \leq n; i++ \)) do
4. \hspace{2em} \( E(b_{ij}) = g^{b_{ij}r^N} \mod N \)
5. \hspace{1em} End For
6. \hspace{1em} End For
7. Return \( E(b_{ij}) \);

As a number of applicants located in the sensing region, most of them can provide feedback results of different grids to the publisher, so the applicant who wants to participate in crowdsensing can utilize Algorithm 2 to encrypt his own matrix. Then these applicants send encrypted matrixes to the authorized agency, and then the authorized agency can calculate the matching of matrixes from the publisher and applicants to allocate the task of crowdsensing in confidentiality.

### 3.5 The Process of Information Conduct (The Authorized Agency)

The authorized agency is the central entity for the task allocation and the central entity for privacy preservation, so most of the management (such as the grids matching and the message sending) is conducted in this entity. Once the authorized agency received the matrix from the publisher and matrixes from various applicants, he calculates the encrypted matrixes with the feature of Paillier encryption system, and gets the matched
matrix $E(C) = E(A) \cdot E(B_1) \cdot E(B_2) \cdot \ldots \cdot E(B_i)$, where $E(C) = E(c_{ij})$. Then the matching matrix $E(C)$ is sent to the publisher, and checked by the publisher to confirm whether this matrix satisfies the request. The algorithm of tasks matching with privacy preservation can be seen in Algorithm 3.

**Algorithm 3**: The tasks matching with location privacy preservation

**Input**: The location matrix $E(a_g)$, the matrix of applicants located in $E(b_g)^k$

**Output**: The feeding back matrix with the secret calculation $E(c_{ij})$

1) For (j=0;j<=n;j++) do
2) For (i=0;i<=n;i++) do
3) $E(c_{ij}) = E(a_g) \cdot E(b_g)^1 \cdot E(b_g)^2 \cdot \ldots \cdot E(b_g)^k$;
4) End For
5) End For
6) Return $E(c_{ij})$;

Once the publisher received the result matrix $E(C)$, he had to decrypt this matrix with the private key of Paillier encryption system. Then the publisher checks whether the non-zero elements in this matrix cover all the grids that the publisher needs. If so, this matrix can provide feedback results of his needs and the publisher asks the authorized agency to collect the results. Otherwise, he has to ask the authorized agency to release this request to applicants again, and asks the authorized agency to find other applicants for crowdsensing.

### 4 Security and Feasibility Analysis

During the process of task allocation in crowdsensing, the information about personal location is submitted by two entities (the publisher as well as applicants). So in order to analyze the security of the proposed scheme thoroughly, we should consider the security of sending the request of crowdsensing from the publisher as well as the security of sending the response for applying the task from applicants. That is, we should ensure the privacy of two entities of the publisher and the applicant cannot be obtained by others.

#### 4.1 The Security of Authorized Agency

For the security of the authorized agency, as this entity is mainly used for allocating the sensing task and transferring the sensing request or the sensing result, this entity will have a lot of chances to get the privacy of the publisher or applicants. But in EGMS, the authorized agency can just receive encrypted matrix $E(A)$ from the publisher and a set of encrypted matrix $E(b_g)^k$ from applicants. The matrix $E(A)$ and $E(b_g)^k$ are encrypted by the public key $pk = (N, g)$, so without the private key $sk = (p, q)$ the authorized agency
can just obtain an encrypted matching result $E(C)$ and he cannot decrypt this matrix to
get the real result of matching matrix $C$. So in EGMS, the authorized agency will get
nothing private about both the publisher and applicants.

4.2 The Security of Publisher

During the process of task allocation in crowdsensing, the threat of privacy violation for
publishers will come from two entities, i.e. the authorized agency as well as applicants. For
one thing, the authorized agency has to check whether grids of feeding back results satisfy
the request of the publisher and in this process the authorized agency may get the precise
location of the publisher requires. For another, applicants also want to know the grids that
the publisher wants to get feedback results. So a privacy preservation scheme has to pre-
vent these two types of entities from obtaining the location privacy. In fact, EGMS can pro-
vide the privacy preservation service for the publisher, and the security can be elaborated
from two aspects. For resisting the privacy violation by the authorized agency, in EGMS,
the information that the authorized agency gets is just the encrypted matrix $E(A)$, and with-
out the private key $sk = (p, q)$ no one can decrypt the confidential elements in this matrix,
let alone the precise location of the publisher wants to get the feedback result. In addition,
even though the authorized agency gets the public key of this publisher, the authorized
agency also difficult to encrypt a number to collide with the precise number that used to
identify the grid that needs to be sensing. This is because different numbers can be used to
denote the grid which the publisher requires to get feedback result. For the privacy violation from applicants, this type of entity is also difficult to get the
precise location of the publisher, as there is no interaction about information between the
applicant and the publisher except the public key. Furthermore, if an applicant wants to
leverage his own location grid to infer the region of the publisher wants to get feedback
result, the result will be distorted and difficult to identify. Because the applicant can just
sense the result from the grid that he located in, but the region that the publisher wants to
get feedback result may be even larger and sometimes will contain a lot of grids. Suppose
that, the number of grids that the publisher wants to get feedback result is denoted as $k$,
and the number of grids that the applicant can sense is $n$ (where $k \gg n$), the probability of
the applicant located in the grid that the publisher needs is $n/k$. If the number of $k$ is large
enough, it is difficult for the applicant to infer the whole region of sensing, as the publisher
can add redundant grids to generalize the real grid or the number of grids that he wants is
larger. In addition, if the applicant can obtain the incentive from the authorized agency, the
applicant also just knows that he is located in a grid that the publisher wants to get result
but not the whole region of crowdsensing. If the applicant does not obtain the incentive, it
will be even difficult to judge whether he is located on the grid that the publisher wants to
get feedback result. Thus, we can conclude from the analysis mentioned above that it is dif-
ficult for an applicant to infer the privacy of the publisher by his own location, even though
he has provided sensing result in crowdsensing.

4.3 The Security of Applicants

In the process of crowdsensing, an applicant usually wants to get the incentive from the
publisher, but does not want his precise location released to any entity (such as the pub-
lisher and the authorized agency). So during the process of confidential crowdsensing, the
location privacy of each applicant needs to be preserved and not be released to both the publisher and the authorized agency. With regard to the confidentiality of EGMS, as the matrix of the applicant is also encrypted by the public key of Paillier encryption system and without the private key \( sk = (p, q) \) no one can decrypt the confidential elements in the matrix. Without the private key, no information about the precise location of the applicant can be released during the process of matrix matching. As a result, if the authorized agency is curious about the privacy of the applicant, EGMS can provide the service of privacy preservation for the applicant against the attack from the authorized agency.

In order to analyze the resistance of EGMS against attacks from the publisher, we assume that during the whole process of crowdsensing all information about the applicant is not sent to the publisher directly, and the publisher can just know the sensing result in the set of feedback results. In the process of task allocation, encrypted matrixes \( E(b_{ij})^k \) are sent from various applicants to the authorized agency, and then the authorized agency calculates the matrix matching with another encrypted matrix \( E(A) \) sent from the publisher, so during this process no information about the applicant is sent to the publisher. In addition, it is not certain about the applicant who provides which encrypted matrix, and the grid that the applicant can provide in the encrypted matrix is also ambiguous, as the process of task allocation is achieved by the encryption matrix matching. As a result, without the private key, the authorized agency knows nothing about the applicant, let alone the publisher, as no information about the applicant is sent to the publisher directly. Thus, with the help of EGMS, the privacy of the applicant is preserved, and any entity such as the publisher and the authorized agency cannot get the privacy of the applicant.

### 4.4 Feasibility Analysis

For the feasibility of EGMS, based on algorithms 1–3, we can see the time complexity of each algorithm is \( O(n^2) \). In addition, as the matrix encryption of the publisher and applicants can be finished offline, the whole process of EGMS is determined by the calculation of encrypted matrix matching in the authorized agency. Suppose that the publisher needs \( k \) applicants in privacy preservation crowdsensing, and then the time complexity of EGMS is determined by algorithm 3, so the time complexity is \( kO(n^2) = O(n^2) \), i.e. the whole time complexity is \( O(n^2) \). However, as the grid matching is calculated by the summation of elements in different matrixes, if the authorized agency can parallel the summation with each element at the same time, the time complexity will be further condensed and reached \( O(1) \). So we can conclude that EGMS can be used in the real environment.

In conclusion, based on the security and feasibility analysis mentioned above, we can regard that during the whole process of crowdsensing with EGMS, and there is no plaintext information about each other interacted with three entities included in the crowdsensing system. Therefore, EGMS can provide the service of privacy preservation in the process of task allocation in the crowdsensing.

### 5 Experimental Verification

#### 5.1 Experiment Settings

In order to verify the performance of our proposed scheme EGMS(such as the execution efficiency as well as the effectiveness of privacy preservation), in the experimental
environment, several groups of experiments are given. Then in the following section, the results and reasons analysis are also given to further demonstrate the conclusion that we got in the security analysis. The simulation experiment is implemented on a laptop with I7 1.80 GHz CPU, 8Gb memory and Windows 10 operation system, and we utilize Python 3.6 to test the algorithm proposed in this scheme and algorithms proposed from other references. The location data used in our simulation comes from Geolife, and we select the same region to generate the grids. Then we assume one out of ten users can feed back the result and can be seen as an applicant. Schemes used in comparison include the scheme of DPLP [12] which is based on the conception of differential privacy, the scheme of PAPP [13] which is based on the conception of path adjust, the scheme of differential-distortion [20] which is based on the conception of location distortion. Therefore, the results and reasons analysis are based on comparisons and analysis with these schemes. For evaluating the performance of execution efficiency, the running time, the matching probability of crowdsensing locations as well as the accuracy of feeding back results are used. For evaluating the performance of effectiveness of privacy preservation, we leverage the success ratio of guessing real locations and the value of entropy of information disclosure.

5.2 Experimental Results and Cause Analysis

In the aspect of evaluating the performance of execution efficiency, we mainly focus on the running time, the matching probability of crowdsensing locations as well as the accuracy of feeding back results. Thus, we assume in the simulation experiment all users in the crowdsensing are applicants that can feed back results to the authorized agency to obtain the incentive, and then we first simulate the running time of each scheme and get the comparison result. In general, the running time is calculated by the time from sending the request of crowdsensing to receiving the feedback result. Figure 3 shows the results of running time of various schemes. In this figure, compared with other schemes, we can see that, though EGMS utilizes the encryption system in calculating the process of confidential matrix matching, the running time of this scheme is shorter than other schemes.

![Fig. 3 The running time of various schemes](image_url)
The reason for this phenomenon can be concluded as the process of encryption or decryption can be conducted offline by the publisher or the applicant, and the authorized agency just implements additive operation on the basis of confidentiality. In addition, why the running time of EGMS is shorter than others also contains the following reasons. Firstly, matrix matching is calculated by the multiplication of matrix dot, which is less complex than matrix multiply, so the time complexity is much less than $O(n^3)$. Secondly, the process of matrix matching is focused on the non-zero element, but not the precise value, so during the process of matrix matching, the operation of XOR can be used to replace the multiplication of matrix dot, which can save much more time during the calculation. Thirdly, the number of grids is limited, so that the size of the matrix is restricted to a certain scale, and a small size of matrix also reduces the complex of calculating the element multiplication. For the running time of other schemes, as these schemes usually leverage adds dummy to satisfy the differential privacy to affect the result of location matching, or convert the road path during the process of data transmission, the running time of these schemes is higher than EGMS. This is because the calculation of adding dummies or the calculation of location shifting will increase the processing step of crowdsensing, and more steps of calculation usually bring more running time.

Figure 4 shows the matching probability of crowdsensing locations of various schemes. In this figure, we can see that the scheme of EGMS performs better not only in the higher probability of matching, but also performs better in the stability of algorithm. The reason for this phenomenon can be summarized as the EGMS does not need to distort the location of the publisher or the applicant or add dummy to generalize the real location. During the whole process, all operations are just the location encryption and decryption, and no other location added in the calculation of location matching, so the matching probability is higher than other schemes (such as the scheme with dummy addition, the scheme with location transformation, the scheme with location distortion).

Figure 5 shows the accuracy of feeding back results of various schemes. In this figure, we can see the accuracy of feeding back results of EGMS is higher than other schemes. As there is no dummy added and no location distortion used in preserving the

Fig. 4 The matching probability of crowdsensing locations of various schemes
location privacy of the publisher and the applicant, all results are calculated by the precise grid of requiring and sensing. Thus, based on the feature of encryption, the scheme of EGMS performs the best among all schemes used in comparison, as other schemes usually utilize dummy addition or location transformation or location distortion which will mislead the accuracy of feedback result.

For evaluating the performance of effectiveness of privacy preservation, we utilize the success ratio of guessing real locations and the value of entropy of information disclosure as metrics, and all results of comparison are based on the above two aspects. Figure 6 shows the success ratio of guessing real locations. From this figure, we can see that for all schemes except EGMS, along with the increasing number of applicants in the task allocation, the risk of successfully identified by an adversary is gradually decreasing. This is because more applicants will generalize the precise location of each other and the adversary
will be difficult to successfully identify the specified user among similar applicants. However, the increasing number of applicants does not affect the performance of EGMS, as this scheme utilizes encryption to conduct the confidential matrix matching which does not depend on the obfuscation of the generalized locations. In addition, as no one can get the precise location without the private key of Paillier encryption system, the adversary cannot guess anything meaningful for any entity, and this feature further increases the privacy preservation level of EGMS.

In general, entropy is usually used for measuring the uncertainty of a result in an information environment. So it can be used as a metric to measure the uncertainty of an adversary guessing the precise location of a user. Suppose that the success ratio of an adversary identifies a special user is \( p(i) \), and based on the equation of entropy we have \( H(i) = -\sum_{i=1}^{n} p(i) \log_2 p(i) \), where \( H(i) \) denotes the uncertainty of this special user. Then based on the principle of maximum entropy, we can conclude that the higher value of entropy the higher uncertainty of the adversary identifies the real locations, the more secure of the personal privacy of the publisher and the applicants. Thus, based on the value of entropy, we measure the performance of privacy preservation with this metric and show the result of comparison in Fig. 7.

Figure 7 shows the entropy of information disclosure of various schemes. From this figure, we can see that the entropy value of EGMS is the highest. This is because all process steps of this scheme are conducted in a confidential environment, and no information about each entity is released to any entity, so that the uncertainty of the adversary is the highest and the information disclosure is the lowest one among these schemes. For other schemes (such as the scheme with dummy addition, the scheme with location transformation, the scheme with location distortion), as they are derived from the conception of generalization or the conception of obfuscation, dummies or distortion locations are used to achieve above operations. But dummies or distortion locations will bring in attribute correlation, and the correlation will be used by the adversary to increase the success ratio of identifying the real location. As a result, these schemes have lower values of entropy than EGMS and performance worse than EGMS, which in turn provides a lower level of privacy preservation for the publisher and the applicant.

---

**Fig. 7** The entropy of information disclosure of various schemes
In conclusion, based on comparisons with other schemes, we can conclude that EGMS performs better than other similar schemes, no matter in the performance of execution efficiency or in the performance of effectiveness of privacy preservation, so it can be used in the actual environment.

6 Related Works

In order to cope with the problems of privacy preservation in crowdsensing, researchers have proposed several groups of explorative research. Based on the difference of system architecture, these research results can be briefly classified into two types, such as the strategy of central architecture and the strategy of distributed architecture. In this section, we will analyze algorithms proposed in recent 5 years in these two strategies that are similar to our proposed EGMS, and then give the advantages and disadvantages of these algorithms. So the following subsection will be divided into the strategy of central architecture and the strategy of distributed architecture.

6.1 The Strategy of Central Architecture

In this architecture, a trusted or semi-trusted entity is used to provide the service of privacy preservation. With this entity, the publisher and applicants will no longer directly interact with each other, so the privacy will be concealed by the disposition of this entity. Based on this strategy, Wang et al. [23] utilized a center server to provide the geo-indistinguishable with differential privacy, so the precise location of each applicant will be difficult to identify, as the adversary was difficult to distinguish the real location from noises. Then Wang et al. [5] further improved this algorithm with the conception of both k-anonymity and ε-indistinguishable, so the applicants will obtain a safety incentive and the willingness of applicants to participate in sensing will be promoted. Yang et al. [17] utilized the density of sensing applicants to construct the indistinguishable of their locations, so as to preserve the personal location privacy of applicants. Wang et al. [24] divided applicants into different groups and utilized the local ε-indistinguishable to establish a larger anonymous region to provide location privacy preservation service for more applicants. Luo et al. [13] adjusted the trajectory path of each applicant, so as to generalize the real path and protect the sensing location of applicants in mobile crowdsensing. Ni et al. [25] utilized a re-encryption scheme to protect the privacy of each entity in crowdsensing, and utilized the generalized results sending to further protect the location privacy of the applicants. Niu et al. [26] proposed a ε-indistinguishable scheme for real time trajectory that generated by the mobile applicant. Wang et al. [20] utilized the model of differential privacy and location distortion to protect the location privacy of applicants in a condition of sparse distribution. Zhang et al. [10] utilized the overlapped strategy of disturbance to provide a better privacy preservation for entities in the process of crowdsensing.

Algorithms of this strategy will have a better performance in the efficiency of privacy providing, as the capacity of center server or agency that can find more anonymous applicants and noises in a short time and guarantee the time-efficient of task allocation and the result feedback. However, as all privacy preservation dispositions are executed by this entity, if it is breached by the adversary or provides preservation...
service for a large number of users in an instantaneous time, this server will become a focus of attacks and the bottleneck of service. As a result, algorithms of this strategy are better to be used in the requirement of higher efficiency of privacy providing, but not the requirement of higher privacy preservation.

6.2 The Strategy of Distributed Architecture

In this architecture, the process of disposing private information in crowdsensing is no longer needed for the center server, but with the collaboration of applicants with each other. With this architecture, Liu et al. [27] provided a scheme of security bidding to select the applicant to conceal others, and during this process other applicants also had no chance to learn the precise location of each other. Yang et al. [18] utilized the character of privacy preservation and the distribution of blockchain, and they also added the completion ratio of tasks to further improve the usefulness of applicants. Tao et al. [28] utilized the scheme of blind signature to guarantee the accuracy of sensing result and the feedback of incentive. Yuan et al. [21] divided the applicants’ region with their attributes, and utilized the scheme of attribute encryption to select applicants and the scheme of symmetric encryption to transfer the sensing result, so that these applicants can be generalized with each other and release no personal location privacy to others. Zou et al. [15] utilized the region obfuscation of users in blockchain, and provided a scheme to provide privacy preservation service for both the publisher and applicants simultaneously. Sun et al. [29] achieved the $\varepsilon$-indistinguishable of applicants with blockchain and double disturbance, so as to enhance the level of privacy preservation. Zhang et al. [30] utilized the difference of sensing space and zero knowledge proof of sensing result to complete the process of privacy preservation task allocation. Zhao et al. [7] provided a rectified scheme for privacy preservation, so beside the privacy preservation of both entities, the publisher can also obtain a better quality of feedback result.

As the process of finding anonymous users or adding noises is provided by applicants with each other, algorithms of distributed architecture no longer need the additional entity, such as the center server or agency, so they can avoid the problems of focus of attacks and the bottleneck of service. However, no matter of schemes of blockchain or zero knowledge proof, they all need the applicants to spend more time in the process of communicating or calculating the parameters in encryption with each other, so algorithms of this type are better to be used in the field of less requirement of service efficiency and the situation of the center server or agency is un-trusted.

7 Conclusion and Future Works

In order to cope with the privacy problem in the task allocation in crowdsensing, in this paper, an encrypted grids matching scheme that is based on the Paillier encryption system has been proposed. We first elaborate on the implementation of our proposed scheme with three algorithms conducted by three entities in the crowdsensing respectively. Then we analyze the security of the proposed scheme from the perspective of the publisher and the perspective of the applicant, which further illustrates the effectiveness of our proposed scheme. Finally, several groups of comparison experiments are given, and results with reasons analysis are also given to further verify the superiority of our proposed scheme.
Though the scheme mentioned in this paper can provide privacy preservation service for the publisher and the applicants, this scheme still has some inherent problems not resolved effectively. For example, if there are fewer applicants than the request of task allocation, how many times and how long is the interval of resubmitting the same request? If the applicant sends a fake result, what kind of punishment is the authorized agency can implement to this applicant? So the future works will be focused on how to solve the problems mentioned above.

Acknowledgements We would like to present our thanks to anonymous reviewers for their helpful suggestions. This work was supported by the Natural Science Foundation of Heilongjiang Province of China under Grant LH2020F050, National Natural Science Foundation of China (No. 61872204). Science Research project of Basic scientific research business expenses in Heilongjiang Provincial colleges and universities of China (No. 135309453).

Author Contributions XdZ gave the idea, LZ and BW did the experiments, XdZ and QY interpreted the results, XdZ wrote the paper.

Funding The Natural Science Foundation of Heilongjiang Province of China under Grant LH2020F050, National Natural Science Foundation of China (No. 61872204). Science Research Project of Basic Scientific Research Business Expenses in Heilongjiang Provincial Colleges and Universities of China (No. 135309453).

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Zhang, L., Liu, D., Chen, M., Li, H., Wang, C., Zhang, Y., & Du, Y. (2021). A user collaboration privacy protection scheme with threshold scheme and smart contract. Information Sciences, 560, 183–201.
2. Huang, P., Zhang, X. N., Guo, L. K., & Li, M. (2021). Incentivizing crowdsensing-based noise monitoring with differentially-private locations. IEEE Transactions on Mobile Computing, 20(2), 519–532.
3. Zhang, L., Chen, M., Liu, D., He, L., Wang, C., Sun, Y., & Wang, B. (2020). A ε-sensitive indistinguishable scheme for privacy preserving. Wireless Networks, 26(07), 5013–5033.
4. Vergara-Laurens, I. J., Jaimes, L. G., & Labrador, M. A. (2017). Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. IEEE Internet of Things Journal, 4(4), 855–869.
5. Wang, Y., Cai, Z., Tong, X., Yang, G., & Yin, G. (2018). Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems. Computer Networks, 135, 32–43.
6. Zhang, L., Li, J., Yang, S., & Wang, B. (2017). Privacy preserving in cloud environment for obstructed shortest path query. Wireless Personal Communications, 96(2), 2305–2322.
7. Zhao, C., Yang, S. S., & McCann, J. A. (2021). On the data quality in privacy-preserving mobile crowdsensing systems with untruthful reporting. IEEE Transactions on Mobile Computing, 20(2), 647–661.
8. Sadhu, V., Zonouz, S., Sritapan, V., & Pompili, D. (2021). CollabLoc: Privacy-preserving multi-modal collaborative mobile phone localization. IEEE Transactions on Mobile Computing, 20(1), 104–116.
9. Shu, J., Jia, X., Kan, Y., & Hua, W. (2018). Privacy-preserving task recommendation services for crowdsourcing. IEEE Transactions on Services Computing, 99, 1–1.
10. Zhang, Y. H., Li, M., Yang, D. J., Tang, J., Xue, G. L., & Xu, J. (2020). Tradeoff between location quality and privacy in crowdsensing: An optimization perspective. IEEE Internet of Things Journal, 7(4), 3535–3544.
11. Zhang, L., Yang, S., Li, J., & Yu, L. (2018). A particle swarm optimization clustering-based attribute generalization privacy protection scheme. Journal of Circuits, Systems and Computers, 27(11), 641–654.
12. Wei, J., Lin, Y., Yao, X., & Zhang, J. (2019). Differential privacy-based location protection in spatial crowdsourcing.
13. Luo, G. C., Yan, K., Zheng, X., Tian, L., & Cai, Z. P. (2020). Preserving adjustable path privacy for task acquisition in mobile crowdsensing Systems. *Information Sciences, 527, 602–619.*
14. Xu, J., Cui, B. J., Shi, R. S., & Feng, Q. L. (2020). Outsourced privacy-aware task allocation with flexible expressions in crowdsourcing. *Future Generation Computer Systems-the International Journal of Exsience, 112, 383–393.*
15. Zou, S. H., Xi, J. W., Wang, H. G., & Xu, G. A. (2020). CrowdBLPS: A blockchain-based location-privacy-preserving mobile crowdsensing system. *IEEE Transactions on Industrial Informatics, 16(6), 4206–4218.*
16. Zhu, X. J., Ayday, E., & Vitenberg, R. (2021). A privacy-preserving framework for outsourcing location-based services to the cloud. *IEEE Transactions on Dependable and Secure Computing, 18(1), 384–399.*
17. Yang, M. M., Zhu, T. Q., Xiang, Y., & Zhou, W. L. (2018). Density-based location preservation for mobile crowdsensing with differential privacy. *IEEE Access, 6, 14779–14789.*
18. Yang, M., Zhu, T., Liang, K., & Zhou, W. (2019). A blockchain-based location privacy-preserving crowdsensing system. *Future Generation Computer Systems-the International Journal of Exsience, 94, 408–418.*
19. He, Y. Y., Ni, J. B., Niu, B., Li, F. H., & Shen, X. M. (2020). Privbus: A privacy-enhanced crowdsourced bus service via fog computing. *Journal of Parallel and Distributed Computing, 135, 156–168.*
20. Wang, L. Y., Zhang, D. Q., Yang, D. Q., Lim, B. Y., Han, X., & Ma, X. J. (2020). Sparse mobile crowdsensing with differential and distortion location privacy. *IEEE Transactions on Information Forensics and Security, 15, 2735–2749.*
21. Yuan, D., Li, Q., Li, G. L., Wang, Q., & Ren, K. (2020). PriRadar: A privacy-preserving framework for spatial crowdsourcing. *IEEE Transactions on Information Forensics and Security, 15, 299–314.*
22. Zhao, Z. J., Ying, Z. B., Yang, Z., Liu, X. M., & Ma, J. F. (2020). Recommendation of platoon members by combining the blockchain and vehicular social network. *Journal of Xidian University, 47(5), 122–129.*
23. Wang, L. Y., Yang, D. Q., Han, X., Wang, T. B., Zhang, D. Q., Ma, X. J., & Acm. (2017). Location privacy-preserving task allocation for mobile crowdsensing with differential geo-obfuscation. *Peer-to-Peer Networking and Applications, 12(5), 1097–1109.*
24. Ni, J. B., Zhang, K., Xia, Q., Lin, X. D., & Shen, X. M. (2020). Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing. *IEEE Transactions on Mobile Computing, 19(6), 1317–1331.*
25. Niu, X., Huang, H. Y., & Li, Y. T. (2020). A real-time data collection mechanism with trajectory privacy in mobile crowd-sensing. *IEEE Communications Letters, 24(10), 2114–2118.*
26. Tong, L., Zhu, Y., Wen, T., & Yu. J. (2018). Location privacy-preserving method for auction-based incentive mechanisms in mobile crowd sensing. *Computer Journal, 61(6), 937–948.*
27. Tao, D., Wu, T. Y., Zhu, S. J., & Guizani, M. (2020). Privacy protection-based incentive mechanism for mobile crowdsensing. *Computer Communications, 156, 201–210.*
28. Sun, Z., Wang, Y., Cai, Z., Liu, T., Tong, X., & Jiang, N. (2021). A two-stage privacy protection mechanism based on blockchain in mobile crowdsensing. *International Journal of Intelligent Systems, 36(5), 2058–2080.*
29. Zhang, J. W., Yang, F., Ma, Z., Wang, Z. Z., Liu, X. M., & Ma, J. F. (2021). A decentralized location privacy-preserving spatial crowdsourcing for internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems, 22(4), 2299–2313.*

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Xiaodong Zheng received the B.E. in Department of mathematics at Anshan Normal University, Liaoning, China, in 2004. She received the M.E. in College of Computer Control and Engineering, at Qiqihar University, Heilongjiang, China, in 2007. She is currently pursuing a Ph.D. degree in the College of Computer science and Technology from Harbin Engineering University. She is also a lecturer in College of Computer Control and Engineering, at Qiqihar University. Her research interests are security and privacy in vehicle networks, mobile privacy protocol and privacy of crowdsensing.

Qi Yuan is currently a professor and graduate study supervisor of College of Communication and electronic engineering at Qiqihar University, China. She received the B.S. degree from Heilongjiang University, China, in 1995, and the M.S. degree from Capital Normal University, China, in 2007. She received the Ph.D. degree in Computer Science and Technology from Harbin Engineering University. Her research interests include information security, and block chain technology.

Bo Wang received the M.S. degree in Computer Application Technology from the Institute of Computer and Control Engineering, Qiqihar University, Qiqihar, China, in 2004. He received the Ph.D. in 2021 in College of Computer Science and Technology at Harbin Engineering University. He is a visiting scholar at the Aerospace Software Engineering Center of Harbin Institute of Technology, Harbin in 2013. His research interests include bioinformatics and multivariate statistical analysis.
Lei Zhang was born in 1982, received the B.E., M.E. in College of Information Science and Electronic Technology at Jiamusi University, Jiamusi, China, in 2005 and 2011, respectively. He received the Ph.D. in 2018 in College of Computer Science and Technology at Harbin Engineering University. He is also a professor and the director of computer software teaching and research office in College of Information Science and Electronic Technology at Jiamusi University. His research interests are security and privacy in vehicle networks, and mobile privacy protocol.