A PCQP Technique Of Location Based Service To Improve k-NN Search Using Secret Circular Shift

[1]B.LEKSHMI JAIN,[2]R.S SYAM DEV,[3]M. MADAN MOHAN

Abstract—**Location based service is a service which allows the user to receive service based on geographic location.The user privacy issue becomes the most important concern, while considering the challenges to establish LBS. The LBS provider has no knowledge about the user's location during the query process. The process of privacy preserving LBS is to provide accurate query results about the** k**-nearest neighbors (k-NN). The proposed novel private circular query protocol (PCQP) which is mainly used to improves the accuracy of k-NN search and protect the query privacy from disclosure without the aid of TTP. It consists of a space filling curve and a public key homomorphic cryptosystem. Initially to form a circular structure, we connect the points of interest (POIs) on a map with the aid of a Moore curve and then the homomorphism of Paillier cryptosystem is used to perform secret circular shifts of POI-related information (POI-info)which is stored on the server side. During the query process after shifting the POI-info and the amount of shifts are encrypted, the actual location is hidden from LBS providers (e.g., servers). Hence the protocol can resist correlation attack and support a multiuser. Thus the resultant analysis shows the security level of the proposed protocol is close to perfect secrecy without the aid of a trusted third party and simulation results show when k is large, the k-NN query accuracy rate of the proposed protocol is higher than 90% .**

***Index Terms*—k-nearest neighbor, location-based service, paillier encryption, privacy preserving, space filling curve.**

I. INTRODUCTION

In recent times, the number of smart phones or mobile devices is increasing rapidly. So the mobile devices and remote server leads to the popularity of mobile network and the soaring trends of cloud computing in which people can enjoy the convenient life experiences offered. For gaining services, one of the popular services is LBS (e.g., Google Map) is introduced in which users can utilize the geographical information. Users often enquire location related questions such as "Where is the nearest police station?" or "Are there some 3-star shop around me?." For activating the LBS, Users have to upload their current locations to the remote provider. However, this actionmight harm the privacy of the user by disclosing the user's current preserving LBS are: *security*and*accuracy*(in k-NN search). There are two major types of research works dealing with the predescribed challenges in the k- NN search of LBS which can be classified into 3-tier and 2-tier LBS architectures. The 3-tier architecture hides user's location TTP.First, in these approaches, a TTP is must for hiding the location of user.The TTP knows too much sensitive information about the user and becomes a single point to be attacked. Second, the cloaking based status [1]–[6] illustrate the situation of being attacks. In a cloaking technique, the querying user is anonymized in the cloak region with the security level of K-anonymity, which means that no one can decide the querying user from other K-1 user in the cloak region. But cloaking technique is breakable by the Background Knowledge Attack. For illustration, if a female user Alice is querying for the nearest women hair salon and the other K-1 user in the cloak region are all happened to be male. Then, server can detect the query is issued from Alice with high probability. Furthermore, the cloaking techniques are also vulnerable to Correlation Attack. For example, server can slender down the size of cloak region by analysing the history or trajectory of user's continuous queries, like "informing me the nearest rest stop coming up along the highway every 9 minutes in the next 50 minutes." An alternative research works of 2-tier architecture [8]–[10], utilizes Private Information Retrieval (PIR) technique to hide the user's location without the help of TTP. The PIR-based technique can counterattack the Background Attack and Correlation Attack. In the most evocative research work [9], the accuracy of k-NN search is near to 100% when k=1 however, it will drop when k increases.

Therefore, on the basis of connected space-filling curves and hormomorphic cryptosystems, an actual secure k-NN search protocol, *Private Circular Query Protocol* (PCQP), is suggested to deal with two challenges. In PCQP, the Moore's version of Hilbert curve [11], [12] (or Moore curve in short) is designated as the mapping tool to transform POIs in 2-D space into 1-D space, and the LBS query is resolved in the 1-D distorted space with the proposed *secret circular shift* scheme. The inefficient way of space transformation effort is remunerated only in the initialization phase for building the LBS. The resultant 2-D to 1-D space transformation can be intermittently reused in the following queries.There are two profits for applying the space transformation to POIs. First, the query in the altered space is easier and faster to be carried out than the calculation of Euclidean distances between all POIs and the query position. Second, the transformed space furs the original 2-D coordinates which is able to achieve its goal of privacy preservation.

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

TABLE I
COMPARISONS AMONG DIFFERENT PRIVACYPRESERVING LBS APPROACHES WHERE nDENOTES THE TOTAL NUMBER OF POIs)

Category	3-tier architecture (with trusted third party)		2-tier architecture	
Type	Cloaking-based [1]–[6]	Hilbert-based [7]	PIR-based [9]	Our method
Accuracy of k-NN	$\cong 100\%$	$\cong 80\%$	Drops largely when $k > 1$	$> 90\%$
# of disclosed POI	$\lvert$users in the CR$\rvert \times k$	$2k$	$\sqrt{n_p}$	$3k$
Security level	Vulnerable to Background Knowledge and Correlation Attacks	Vulnerable to Correlation Attack	Robust	Robust

The profits of the proposed protocol are enumerated in the following:

1) Supportive multiuser scenario. The public-key characteristics of Paillier cryptosystem, one of the significant components of our protocol, can easily adapt to the multiuser background. The proposed protocol only requires users to keep their private keys on the client side and send the corresponding public keys to the server side, which decouples the relation among users. The key managing issue of newly joined user can be intuitively resolved by the properties of the approved public key cryptosystem

2) Confliction to Correlation Attack and Background Knowledge Attack. The secret circular shiftis performed before each query and the amount of shift is resolute only by the querying user, which can be regarded as an one-time pad encryption scheme, and therefore, providing high security. Servers cannot deduceany knowledge about the user's location from the query antiquity and the user's sketches, since the amount of shift has been twisted by user. The POI information has also been encrypted. Under such condition, the Correlation Attack and Background Knowledge Attack made by the server cannot succeed.

3) Providing high accuracy k-NN search results. In general, the security challenge and accuracy challenge cannot be mutually addressed. There are lots of mechanism which can obtain accurate k-NN results but are vulnerable to the Correlation Attack [1]–[6]. On the other hand, there are research works providing high security whereas the accuracy of k-NN results dribs largely when$k$>1 [9]. Prominently, the proposed protocol, with some simple modifications, can attain high accuracy rate for k-NN search (larger than 90% even if $k$is large) without conceding the robustness of security.

II. PRELIMINARIES

A. Space-Filling Curves

Space filling curves [12] characterize a class of curves which can pass throughall cells in a 2-D space, or more generally, a multidimensional hypercube, without crossing themselves. Hilbert curve is important member of this class. Hilbert curve is well-known for the ability of partly retaining the neighboring adjacency of the original data.It is showed that Hilbert curves can achieve the best clustering property [13], [14].Fig. 1 illustrate the Hilbert curves of the first three orders, where the N-th order Hilbert curvecan be traversed than or equal to one.

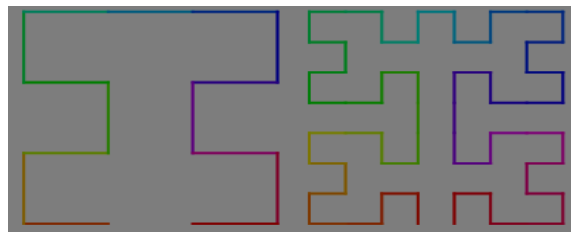


Fig. 1. Moore curve

1) Deviations of Hilbert Curves: According to [11], [12],there are some dissimilarities of Hilbert curves. One can change the configuration of Hilbert curves to construct curves with different starting and ending points. Moore curve, as showed in Fig.1.is one of the Hilbert curve's variations and is approved in our protocol because of its end-point-connected property. The end-point connection property of Moore curve strings all the POIs into a circular structure of locality, and every POI has the neighboring relationship with POIs on both directions of the curve. Due to this circularly connected property, Moore curve is adopted as ansubstantialconstituent to develop a privacy preserving protocol for LBS.

2) *Moore curve*

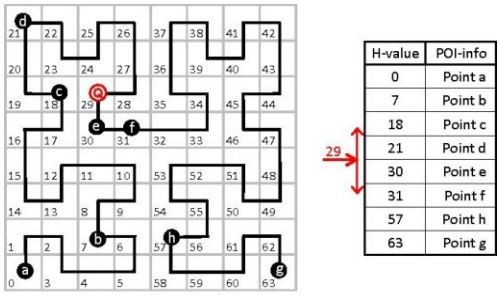
It is a continuous fractal space-filling curve which is a variant of the Hilbert curve. Precisely, it is the loop version of the Hilbert curve, and it may be supposed as the union of four copies of the Hilbert curves combined in such a way to make the endpoints coincide.

B. k-NN Search on Space-Filling Curves

Since Hilbert curves possess superior locality preserving property, they have long been applied to resolve$k$-NN problems. The basic ideas of applying Hilbert curves for k-NN search is familiarised in this section which is based most on the work of [7].

On a map, a Hilbert curve can be well-defined by the curve setting parameters: curve's starting point, curve orientation, curve scale factor and curve order. An N-th order Hilbert curve can fill up a square space (a.k.a. the target map in LBS) with 2N×2N cells, and each cell is given an integer value, called *H-value*.

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET



H-value	POI-info
0	Point a
7	Point b
18	Point c
21	Point d
30	Point e
31	Point f
57	Point h
63	Point g

Fig. 2. (a) 8 POIs are covered by a Hilbert curve of order 3.
(b) The DB contains POI-info and the corresponding H-values.

The accompanying information of POIs are stored in database (or DB in short) on the server side, where one column records the H-values and the other column records the POI-info, such as the real world coordinates of POIs or other exact location information.

Now, if we want to discover the k-NN of the query position Q, with the associated H-value 29 in Fig. 2, the examining will be started at the row in DB whose H-value is nearest to 29 (e.g., the row with corresponding H-value 30). Next, retrieves the data by alternating the search directions in DB iteratively, that is, descending or ascending order of H-value are 21 and 30, respectively. We can see from this example that Hilbert curve based approach may not find the best k-NN results since the ground truth for this work is {c,e}. Notice that there might be two or more POIs having the same H-value if they are inside the same cell of the map. If there are many POIs in a cell, it is just like the resolution of the map is not high enough and many POIs have the same coordinate. It will cause the server unable to determine the distance between the query point and those POIs inside a same cell, because those POIs have the same H-value, and the query accuracy rate will be decreased. There is an experiment conducted in [7] and the number of POIs is suggested to be less than or equal to 2 per cell to acquire better query results. And this assumption is valid in real scenarios since we can choose the order of a Hilbert (or Moore) curve on a map to satisfy this requirement. Let's define (POI)/(cell) as average number of POIs within one cell.

C. Homomorphic Cryptosystem

For successfully conducting our protocol, a homomorphic cryptosystem is indispensable. Traditionally, there will be a TTP playing an important role to hide the user's location in a location-based service. Without a TTP in our protocol, we can take the advantage of homomorphic cyptosystem to prevent user's location information conducting the service in homomorphic encryptiondomainon the LBS- server side. The property of a homomorphic cryptosystem is that some specific algebraic operations on plaintext can be equivalently achieved in the encryption domain by other algebraic operations performed on the ciphertext.

Any homomorphic cryptosystem can be seamlessly integrated with the proposed protocol as long as it has the homomorphic property over addition of two ciphertexts and multiplication of one ciphertext and one plaintext, such as Paillier cryptosystem [15] or NTRU cryptosystem [16], the later one even supports Homomorphic Multiplication of two ciphertexts.

It briefly describes the Paillier cryptosystem where the associated homomorphic property is sufficient to be integrated in the proposed protocol. Of course, further homomorphism properties, e.g., NTRU cryptosystem [16], can assist in building a more efficient protocol.

1) Paillier Cryptosystem: Paillier cryptosystem [15], isa public-key cryptography based on the decisional composite residuosity problem to assure its security. We will use$E_r(m)$ to denote the encryption of message $m \in z_n$ and $D(E_r(m))$ to denote the corresponding decryption, where r a random number is belongs to Z_n and n is a product of two large primes. The essential random number r in the Paillier cryptosystem will foil from generating the same ciphertext of the same plaintext message m, that is, the ciphertext $E_{r1}(m)$ will be totally different to the ciphertext $E_{r2}(m)$.

In the field of secure computation, Paillier cryptosystem is famed for its Additive Homomorphism. That means, for a given public-key k_p and the ciphertexts Er1(m1) and Er2(m2), one can directly compute the adding of plaintexts m_1+m_2 in the encryption domain as:

$$D(Er\ 1(m1).Er2(m2) \bmod n^2) = M_{1+}M_2(1)$$

Paillier also supports Homomorphic Multiplication of one ciphertext and one plaintext, that is, for the given k_p,Er 1(m1) andm1, one can directly compute the multiplication of in the encryption domain by

$$D((Er1(m1)^{m2} \bmod n^2)) = M_{1*}M_2 \qquad (2)$$

D. Circular shift

Operation of rearranging the entries in a tuple, either by moving the final entry to the first position, while shifting all other entries to the next position.Due to the characteristics of Moore curve, the POIs stored in H-table's first and last rows are very close to each other, geographically. That is, despite whatever the H-index distance between the first and the last row would be, the two POI is neighbor to each other in the 2-D space. Following the same inference, the first and the last rows of H-table could be alleged of as linking together just like an edge had been added to

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

connect the two ending points of the corresponding Moore curve.

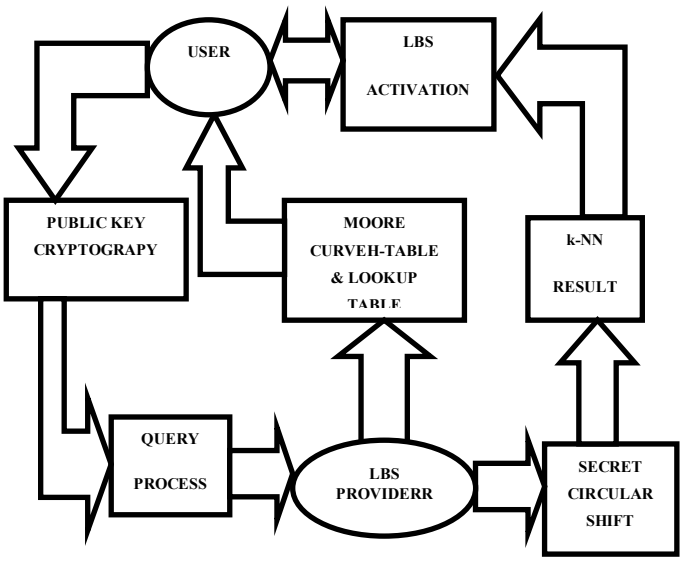


Fig. 3.Private circular query protocol.

III. THE PRIVATE CIRCULAR QUERY PROTOCOL (PCQP)

For achieving privacy preserving LBS, a novel of effective and efficient secure k-NN search scheme, called *Private Circular Query Protocol* (PCQP), is proposed. PCQPnot only can improve the accuracy of k-NN search, but also protect the query privacy from disclosure.

A. Process of PCQP

In PCQP, Moore curves are chosen as the mapping tool and will bring out a new way to query k-NN securely. The whole architecture of PCQP is illustrated in Fig. 3, which belongs to 2-tier LBS architecture category, and the whole protocol consists of the following 6 steps:

Initiating Processes

step-1: Server builds a Moore curve and produces H-indexes for all registered POIs on the target map. In this first step, LBSserver constructs an appropriate Moore curve covering up the target map and builds a table containing all the evident data related to all POIs. Each stored POI in the table (called H-table, thereafter) is totalled according to an evenly dispersed H- index with common difference d instead of the originally associated H-value. The mapping from H-values to H- indexes is kept in a lookup-table on the server. Since the generation of H-indexes needs to be done only once in the server side, the necessary efforts can be treated as a part of the service setup costs.

step-2: Server publicly announces the lookup-table andMoore curve's setting parameters to the registered users so that anenquiring user can compute the H-index of his/her current position on the map. The lookup-table and the Moore curve's setting parameters could be made publicly toevery registered user, and this public announcement won't affect the privacy issue. By the way, a registered user can download this information just from LBSWebsite.

step-3: User chooses his/her public and private key pairs of the Pailler cryptosystem and sends the public key to server.

Enquiry Processes

step-4: User issues a k-NN query to server.

(a) User chooses an $n_p * n_p$,l_1-offset circular shift permutation matrix $(P^{l1}_{i,j})_{(i,j=0\ldots n_{p-1})}$, where n_p denotes the number of POIs in H-table and the($n_p - l_1$) the element of the first row of is the only nonzero element in that row.

(b)User adds a number l_2=d*$l_1$tothe H-index of his/her current site to produce a shifted-H-index.

(c)User sends the shifted-H-index and the scrambled first row of ($P^{l1}_{i,j}$) by the public-key selected in step-3, denoted as, to server and issues a k-NN query.

step-5: Server accomplishes a secret circular shift, which is defined by $Er_{i,j}(P^{l1}_{i,j})$, on the POI-info column of H-table based on the Additive and Multiplicative homomorphisms of Paillier cryptosystem with user's public key. Server, then, conducts a k-NN search upon the circularly shifted H-table, and returns the encrypted examine results back to user.

step-6: User select his/her private key (selected in step-3) to decrypt the received results and finds the required k-NN solutions.

Since H-index of the querying user and the POI-info column of H-table have respectively been added by l_2 and secretly circularly shifted by 1_1 where l_2=d*l_1, the secret k-NN search results done in the shifted H -table will be the same as that of the original k-NN search results done in their plaintext version.

B. Details of PCQP

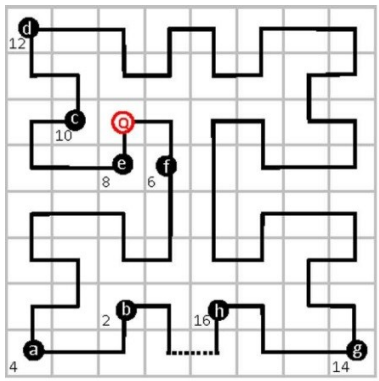
1) H-Index versus H-Value: Observing the Hilbert curveshowed in Fig. 2, one can find that the starting and the ending cells do not neighbor to each other. In this case, if the query position is near to the starting or ending cell of the curve, then the searching directions will be reduced from two to one, which is opposite to the starting or ending cell. Besides, one can also find that those H-values in DB are only used to string all the POIs together in a locality-preserving order and behave as a tool for addressing all POIs in DB. As long as those H-values retain their numerical order, altering those H-values won't affect the result of query because only the order of H-values is of concern in retrieving k-NN search results.

Thus, as predescribed, we adopt Moore curves, instead of the original Hilbert curves, as our 2-D to 1-D

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

mapping tool, to construct POIs into a circular structure of locality. And we change the H-values in DB into an evenly distributed sequence with a common difference d to construct the H-table (as shown in Fig. 4(a) and (c)). This linearly and evenly distributed sequence will facilitate the required circular shift operation. The numbers in the sequence is known as H-indexes. Formally, the H-index of the j-th POI, denoted as poi_j , in a Moore curve can be defined as

$$\text{H-index}(POI_J)=d*j \qquad (3)$$



(a)

Lookup-table	
H-value	H-index
2	2
5	4
16	6
19	8
23	10
26	12
58	14
62	16

(b)

8

H-index	POI-info
2	Point b
4	Point a
6	Point f
8	Point e
10	Point c
12	Point d
14	Point g
16	Point h

(c)

12

H-index	POI-info
2	Point g
4	Point h
6	Point b
8	Point a
10	Point f
12	Point e
14	Point c
16	Point d

(d)

Fig. 4. (a) 8 POIs are covered by a Moore curve of order 3. (b) The lookup -table for identifying the correspondence between H-values and H-indexes. (c) The evenly distributed H-table. (d) The H-table after POI-info column shifting 2 units downward, where the associated querying H-index is $\text{shifted\_}H\text{\_index}(Q)=8+(2\times2)=12$.

where j is the sequencing-order of the POI along with the given Moore curve and d is an integer greater than or equal to one.

1) Secret circular shift in H-table

Notice that, due to thecharacteristics of Moore curve, the H-index distance between the first and the last row would be, the two POIs neighbor to each other in the 2-D space, as shown in Fig. 4(a) and (c). Following the same implication, the first and the last rows of H-table could be supposed to link together just like an edge had been added to connect the two ending points of the corresponding Moore curve.

Let's define an entry (or a row) of H-table as the basic accessible unit; obviously, every index item(including both the first and the last one) has a neighboring relationship between its two adjacent entries. Now, if we circularly shift the POI-info column of H-table two units downward but keep the H-index column unharmed, as shown in Fig. 4(d), and then make a k-NN query at Q. Through the example H-tables presented in Fig. 4(c) and (d), it follows that we need only to circularly shift the querying H-index from 8 to 12, then exactly the same k-NN search results will be obtained, as before. In general, if we want to get the same k-NN query results after shifting the POI-info column t units downward circularly, we just need to change our querying H-index,H-index(Q), to a shifted querying H-index, shifted-H-index(Q)

as

$$\text{Shifted-H-index(Q)} = \text{H-index}+(d*t) \qquad (4)$$

and then send shifted-H-index(Q)to server as the new querying index. Notice that, upward shifting the POI-info column is equivalent to set a negative integer to t.

In addition, our goal is to circularly shift the POI-info column and keep the shift amount secret to the server. Without knowing the shift amount, even though the server knows the Shifted-H-index(Q) is 12, server has no way to figure out what the orginal H-index was. Therefore, server cannot derive user's location from the query information.

Then secret circular shift of H-table's POI-info column in the server side of a position circular shift of a length data vector (e.g., the POI-info column) can be done by multiplying the data vector by an offset *circular shift* permutation matrix, which is defined by

$$\left(P_{i,j}^{t}\right)=\begin{cases}1, & iff\ j=i+\left(n_p-t\right)mod\ n_p\\ 0, & otherwise\end{cases} \qquad (5)$$

In [17], on the basis of Paillier encryption scheme, approach to secretly scramble data vector by multiplying it with a permutation matrix was proposed, in which the permutation matrix is in plaintext version while the data vector is encrypted. Inspired by [17], based also on the Paillier cryptosystem, a new approach for circularly shifting data vector by using encryption domain matrix-vector multiplication will be introduced, where the data vector is in its plaintext version while the elements of the permutation matrix are encrypted.

C. k-NN Search Algorithms in PCQP

1) Adaptive Search Window: In a k-NN problem, the ground truth with respect to a query locations are distributed on the map and could be covered by a sufficiently large 2-D search window.

In order to find the exact k-NN result, we define aadaptivesearch window of size $(2*D+1)^2$, where is the distance between the querying cell and the nearest cell on the borders of the search window. Thus, for applying

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

PCQP to k-NN search, is chosen to be the minimum positive integer satisfying

$(2 *D+1)^2 \geq k$

to guarantee that there are more than or equal to k POIs close to the query location in the search window, under the condition that (POI)/(CELL) ≅ 1.If the full coverage of the predescribed k-adaptive search window could be searched, one would get the exact k-NN result since the coverage of adaptive search window centered at includes more than or equal to k POIs.

2*) Connected-Path Based k-NN Search Algorithm*: Within a k-adaptive search window, the Moore curve can be divided into many disjoint connected paths. And based on the basic search process, the returned POIs from a k-NN search consist of a connected path on the Moore curve. For finding the best neighbors which are covered by a k-adaptive search window, we have to issue k-NN queries at each connected path to achieve the full coverage.

3) *Heuristic Cross-Like k-NN Search Algorithm*:For achieving the full coverage of a given k-adaptive search window in a heuristic way, let's observe some Moore curvecovered by a 3*3 search window. If we issue a 9-NN search at the center of each of the searching windows, under the condition of (POI)/(CELL) ≅ 1 , there are some POIs won't be visited during the query since the H-indexes of the unvisited POIs are too far away from the center (e.g., the cells on the noncenterpassing connected paths) so that they cannot be reached within moves in H-indexes along the center passing connected path.

IV. PERFORMANCE ANALYSIS AND EXPERIMENTAL RESULTS

First, we will demonstrate the accuracy rate of the proposed cross like search algorithm when applied to step-4 in PCQP. Next, we will compare the accuracy performances of the cross-like search equipped PCQP with that of two related works: DCQR [7] and PIR-NN [9] to find the nearest neighbors. Finally, we will also inspect the communication and the computation difficulties, with security concern, of PCQP.

A. Experimental Setup

We implement the proposed PCQP by Java. The performance evaluation of client side is simulated on a PC equipped with Win7 OS, Intel i5-2400 3.1 GHz processor and 10 GB RAM. The LBS is conducted on a server with Debian 64bit OS, 2 Intel Xeon E5420 processor and 32 GB RAM.

We use Sequoia as one of our testing datasets which consists of 62956 real world locations site. We also tested two synthetic datasets, in which two sets of 67536 POIs are uniformly and normally distributed in a square map, respectively. Moreover, the Paillier 1024 bits cryptosystem is taken as our encryption tool. In every one of the following k-NN experiments, we varied k from 1 to 100 and issued k-

NN query on 1000 different locations on the map. Given the returned result set S and the k-NN ground truth, we express the$k$-NN search accuracy rate as (|S∩ T|/|T|)

B. Performance Analysis

Based on both synthetic and real world datasets, compare the accuracy rate of the proposed cross-like search equipped PCQP with two additional queries, with two related benchmark works: DCQR and PIR-NN. Based on the characteristics of those approaches, the sizes of server returned resultant sets (or the numbers of disclosed POIs) for a k-NN query are in DCQR, PIR-NN and cross-like search equipped PCQP, respectively.

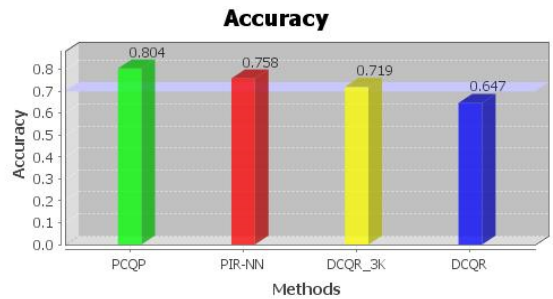


Fig.5. Accuracy measure

Although PIR-NN approach performs well when the value is small, the accuracy performance of PIR-NN drops rapidly when the value is increased, this is because PIR-NN is designed for querying the nearest-neighbor only. The corresponding accuracy evaluationresults on the aforecited real world dataset. Since the geographic distribution of POIs in the real world dataset is not a square but an irregular-shape, we set the order of the curve to 9 such that the area covered by the dataset.

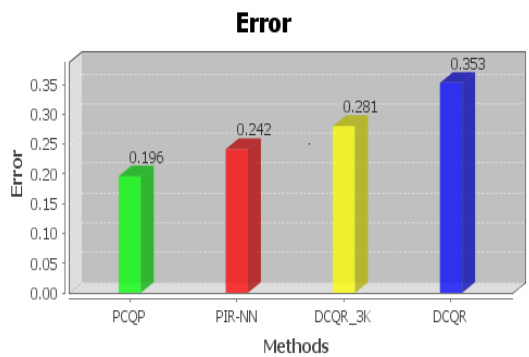


Fig.6. Error measure

The proposed cross-like search equipped PCQP always enhances the accuracy rate about 10% as compared with

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET

other related approaches. In our approach, higher than 90%accuracy rate can always be reached whenpredescribed two more queries are added and error rate decreases when compared to other methods.

V. CONCLUSION

A Private Circular Query Protocol with cross like search mechanism is proposed to simultaneously achieve the location-based k-NN query and the location privacy preservation, in a novel way. This is the first work to apply Moore curves and Pailler cryptosystem to location-based query problem. The security level of the proposed protocol is near to perfect confidentiality without TTP and the accuracy rate is stably above 90% regardless of the variation of k. The proposed circular structure impeccably integrates the robustness of specific public-key cryptosystems and the clustering property of space-filling curves. Thus the proposed protocol has achieved aninnovative computing scheme for conducting clandestine computation with well-clustering property.

REFERENCE

[1]. P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," *IEEETrans. Knowl. Data Eng.*, vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[2]. J.-H. Um, H.-D. Kim, and J.-W. Chang, "An advanced cloaking algorithm using Hilbert curves for anonymous location based service,in*Proc. 2010 IEEE Second Int. Conf. Social Computing*, 2010, pp.1093–1098.

[3]. A.-A. Hossain, A. Hossain, H.-K. Yoo, and J.-W. Chang, "H-star:Hilbert- order based star network expansion cloaking algorithm in road networks," in *Proc. IEEE 14th Int. Conf. Computational Science andEngineering (CSE)*, Aug. 2011, pp. 81–88.

[4]. M. Gruteser, D. Grunwalddepartment, and C. Science, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. 1st Int. Conf. Mobile Systems, Applications andServices*, 2003, pp. 3142.

[5]. C.-Y. Chow, M. F. Mokbel, and W. G. Aref, "Casper*: Query processing for location services without compromising privacy," *ACM Trans. Database Syst.*, vol. 34, pp. 24:1–24:48, Dec. 2009.

[6]. M. Mokbel, "Towards privacy-aware location-based database servers," in *Proc. 22nd Int. Conf. Data Engineering Workshops*, 2006, pp. 93–102.

[7]. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in *Proc. 10th Int. Conf. Advances in Special and TemporalDatabases (SSTD'07)*, 2007, pp. 239–257

[8]. Khoshgozaran, C. Shahabi, and H. Shirani-Mehr, *Location Privacy:Going Beyond k-Anonymity, Cloaking and Anonymizers*. NewYork, NY, USA: Springer-Verlag New York, Inc., Mar. 2011, vol. 26, pp.435–465, no. 3.

[9]. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, Private queries in location based services: anonymizers are not necessary,"in*Proc. 2008 ACM SIGMOD Int. Conf. Management of Data*, New York, NY, USA, 2008, pp. 121–132, ser. SIGMOD'08, ACM.

[10]. S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest neighbor search with strong location privacy," in *Proc. VLDB Endow.*, Sep.2010, vol. 3, no. 1–2, pp. 619–629.

[11]. E. H. Moore, "On certain crinkly curves," *Trans. Amer. Math. Soc.*,vol. 1, pp. 72–90, Jan. 1900.

[12]. H. Sagan, *Space-Filling Curves*. New York, NY, USA: Springer-Verlag, 1994.

[13]. Moon, H. Jagadish, C. Faloutsos, and J. Saltz, "Analysis of the clustering properties of the hilbert space-filling curve," *IEEE Trans. Knowl.Data Eng.*, vol. 13, no. 1, pp. 124–141, Jan./Feb. 2001

[14]. H. V. Jagadish, "Linear clustering of objects with multiple attributes,"in*Proc. 1990 ACM SIGMOD Int. Conf. Management of Data*, New York, NY, USA, 1990, pp. 332–342, ser. SIGMOD'90, ACM.

[15]. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology Eurocrypt 1999*. NewYork,NY, USA: Springer-Verlag, 1999, pp. 223–238.

[16]. J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: A ring-based public key cryptosystem," in *ANTS*, ser. Lecture Notes in Computer Science, J. Buhler, Ed. New York, NY, USA: Springer, 1998, vol. 1423, pp.267–288.

[17]. T. Onodera and K. Tanaka, "Shuffle for paillier's encryption scheme,"*IEICETrans.Fund. Electron.,Commun., Computer Sci.*, vol. E88-A,pp. 1241–1248, 2005.

[18]. D. Kahn, *The Code Breakers—The Story of Secret Writing*. NewYork, NY, USA: Macmillan, 1967.

[19]. S. A. V. Alfred, J. Menezes, and P. C. van Oorschot, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

B. Lekshmijain is a PG Scholarin computer science department at Anna university,Chennai.She received the B.E degree from Sri ShakthiInstitutte of Engineering and technology College, Coimbatore in 2012 and pursuing the ME degree from Ranganathan Engineering College, Coimbatore in 2014.Her area of interest include Network security, Data structure.

R.S SyamDev is an assistant professor at Narayanaguru College of Engineering ,Manjalumoodu. He received the B.E degree from Noorul Islam College of Engineering, Kumaracoil (1995-1999) and the M.E degree from J.J College of Engineering ,Trichi (2005-2007).

M.Madanmohan isan assistant professor at Ranganathan Engineering College, Coimbatore. He received the B.Tech degree from Adhiyamaan College of Engineering, Hosur (2007-2010) and the M.E degree from Anna University of Technology,Coimbatore (2010-2012).

.

ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET