ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Robust and secure PCQP Technique of Location Based Service to Improve K-NN Search Using Secret Circular Shift

Lokireddi Chenna Reddy
M.Tech Student ,
Computer Science Engineering Department,
Sir C R Reddy College of Engineering.

Chalasani Rama Devi
Assistant Professor,
Computer Science Engineering Department,
Sir C R Reddy College of Engineering.

Abstract:

Location-based services (LBS) are a general class of computer program-level services that use location data to control features. As such LBS is an information service and has a number of uses in social networking today as an entertainment service, which is accessible with mobile devices through the mobile network and which uses information on the geographical position of the mobile device.

This has become more and more important with the expansion of the smartphone and tablet markets as well. LBS are used in a variety of contexts, such as health, indoor object search, entertainment, work, personal life, etc. Privacy issues (including security, privacy, and trust) in mobile social networks are concerned about the condition of being protected against different types of failure, damage, error, accidents, harm or any other non-desirable event, while mobile carriers contact each other in mobile and cloud environments. The rationale behind this work paper is to investigate the threats to privacy that come up while users not have a good judgment of privacy consciousness. A successful privacy-preserving LBS must be secure and provide accurate query results. In this paper, we propose a private circular query protocol (PCQP) to deal with the privacy and the accuracy issues of privacy-preserving LBS.

The protocol consists of a space filling curve and a public-key homomorphic cryptosystem.First, we connect the points of interest (POIs) on a map to form a circular structure 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), stored on the server side.

Since the POI-info after shifting and the amount of shifts are encrypted, LBS providers (e.g., servers) have no knowledge about the user's location during the query process. The protocol can resist correlation attack and support a multiuser scenario as long as the predescribed secret circular shift is performed before each query; in other words, the robustness of the proposed protocol is the same as that of a one-time pad encryption scheme.

Keywords:

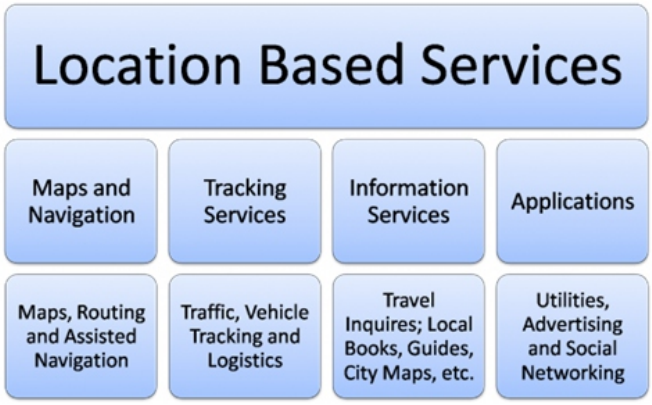
location-based service, Cloud Computing, paillier encryption, privacy preserving, space filling curve, Mobile Networks.

Introduction:

LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine (a.k.a. ATM) or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games. They are an example of telecommunication convergence. This concept of location based systems is not compliant with the standardized concept of real-time locating systems (RTLS) and related local services, as noted in ISO/IEC 19762-5 and ISO/IEC 24730-1. While networked computing devices generally do very well to inform consumers of days old data, the computing devices themselves can also be tracked, even in real-time.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

The main advantage is that mobile users do not have to manually specify ZIP codes or other location identifiers to use LBS, when they roam into a different location. GPS tracking is a major enabling ingredient, utilizing access to mobile web.



Locating methods:

Control plane locating:

Sometimes referred to as positioning, with control plane locating the service provider gets the location based on the radio signal delay of the closest cell-phone towers (for phones without GPS features) which can be quite slow as it uses the 'voice control' channel.

In the UK, networks do not use trilateration; LBS services use a single base station, with a "radius" of inaccuracy, to determine a phone's location. This technique was the basis of the E-911 mandate and is still used to locate cellphones as a safety measure. Newer phones and PDAs typically have an integrated A-GPS chip.

GSM localization:

GSM localization is the second option. Finding the location of a mobile device in relation to its cell site is another way to find out the location of an object or a person. It relies on various means of multilateration of the signal from cell sites serving a mobile phone.

The geographical position of the device is found out through various techniques like time difference of arrival (TDOA) or Enhanced Observed Time Difference (E-OTD).

Self-reported positioning:

A low cost alternative to using location technology to track the player, is to not track at all. This has been referred to as "self-reported positioning". It was used in the mixed reality game called Uncle Roy All Around You in 2003 and considered for use in the Augmented reality games in 2006.

Instead of tracking technologies, players were given a map which they could pan around and subsequently mark their location upon. With the rise of location-based networking, this is more commonly known as a user "check-in".

Another example is Near LBS (NLBS), in which local-range technologies such as Bluetooth, WLAN, infrared and/or RFID/Near Field Communication technologies are used to match devices to nearby services. This application allows a person to access information based on their surroundings; especially suitable for using inside closed premises, restricted/ regional areas.

Another alternative is an operator- and GPS-independent location service based on access into the deep level telecoms network (SS7). This solution enables accurate and quick determination of geographical coordinates of mobile phone numbers by providing operator-independent location data and works also for handsets that are not GPS-enabled.

Privacy issues:

The Location Privacy Protection Act of 2012 was introduced by Senator Al Franken in order to regulate the transmission and sharing of user location data in USA. It is based on the individual's one time consent to participate in these services (Opt In). The bill specifies the collecting entities, the collectable data and its usage.

The bill does not specify, however, the period of time that the data collecting entity can hold on to the user data (a limit of 24 hours seems appropriate since most of the services use the data for immediate searches, communications, etc.), and the bill does not include location data stored locally on the device (the user should be able to delete the contents of the location data document periodically just as he would delete a log document).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

The bill which was approved last month by the Senate Judiciary Committee, would also require mobile services to disclose the names of the advertising networks or other third parties with which they share consumers' locations.

With the passing of the CAN-SPAM Act in 2003, it became illegal in the United States to send any message to the end user without the end user specifically opting-in. This put an additional challenge on LBS applications as far as "carrier-centric" services were concerned. As a result, there has been a focus on user-centric location-based services and applications which give the user control of the experience, typically by opting in first via a website or mobile interface (such as SMS, mobile Web, and Java/BREW applications).

The European Union also provides a legal framework for data protection that may be applied for location-based services, and more particularly several European directives such as: (1) Personal data: Directive 95/46/EC); (2) Personal data in electronic communications: Directive 2002/58/EC; (3) Data Retention: Directive 2006/24/EC. However the applicability of legal provisions to varying forms of LBS and of processing location data is unclear.

One implication of this technology is that data about a subscriber's location and historical movements is owned and controlled by the network operators, including mobile carriers and mobile content providers. Mobile content providers and app developers are a concern. Indeed, a recent MIT study by de Montjoye et al. showed that 4 spatio-temporal points, approximate places and times, are enough to uniquely identify 95% of 1.5M people in a mobility database.

The study further shows that these constraints hold even when the resolution of the dataset is low. Therefore, even coarse or blurred datasets provide little anonymity. A critical article by Dobson and Fisher discusses the possibilities for misuse of location information. Beside the legal framework there exist several technical approaches to protect privacy using privacy-enhancing technologies (PETs). Such PETs range from simplistic on/off switches to sophisticated PETs using anonymization techniques, e.g., related to k-anonymity. Only few LBS offer such PETs, e.g., Google Latitude offered an on/off switch and allows to stick one's position to a free definable location.

Additionally, it is an open question how users perceive and trust in different PETs. The only study that addresses user perception of state of the art PETs is. Another set of techniques included in the PETs are the Location obfuscation techniques, which slightly alter the location of the users in order to hide their real location while still bein able to represent their position and receive services from their LBS provider.

Traditional encryption based techniques incur expensive O(n) computation cost (where n is the total number of points in space) and possibly logarithmic communication cost for resolving a K-NN query.

This is because such approaches treat points as vectors in space and do not exploit their spatial properties. In contrast, we use Hilbert curves as efficient one-way transformations and design algorithms to evaluate a K-NN query in the Hilbert transformed space.

Consequently, we reduce the complexity of computing a K-NN query to and transferring the results to the client in O(K), respectively, where N, the Hilbert curve degree, is a small constant.

Our results show that we very closely approximate the result set generated from performing K-NN queries in the original space while enforcing our new location privacy metrics termed u-anonymity and a-anonymity, which are stronger and more generalized privacy measures than the commonly used K-anonymity and cloaked region size measures.

Existing System:

For building privacy-preserving LBS, there are two major challenges: security and accuracy (in -NN search). There are two major types of research works dealing with the pre-described challenges in the -NN search of LBS which can be classified into 3-tier and 2-tier LBS architectures.

3-Tier Architecture:

The 3-tier architecture hides user's location with the aid of a trusted third party (TTP). There are some drawbacks when we rely the privacy-preserving LBS upon a TTP. First, in these approaches, a TTP is a must for hiding the location of user.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Cloaking technique:

In a cloaking technique, the querying user is anonymized in the cloak region with the security level of -anonymity, which means that no one can distinguish the querying user from other users in the cloak region.

2-Tier Architecture:

The 2-tier architecture, utilizes Private- Information-Retrieval (PIR) technique to hide the user's location without the TTP. The PIR-based technique can resist Background Attack and Correlation Attack.

Disadvantages:

3-Tier Architecture:

- The TTP knows too much sensitive information about the user and becomes a single point to be attacked.

- The anonymized status or space transformed status of a user is breakable by applying the Background Knowledge Attack or the Correlation Attack.
Cloaking technique.

- Cloaking technique is breakable by the Background Knowledge Attack.

- Cloaking techniques is also vulnerable to Correlation Attack. For example, server can narrow down the size of cloak region by analyzing the history or trajectory of user's continuous queries, like "informing me the nearest rest stop coming up along the highway every 5 minutes in the next 30 minutes.

Proposed System:

On the basis of connected space-filling curves and hormomorphic cryptosystems, an effective secure -NN search protocol, Private Circular Query Protocol (PCQP), is proposed. In PCQP, the Moore curve is selected 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 transformed space with the proposed secret circular shift scheme. The time-consuming space transformation effort is paid only in the initialization phase for building an LBS.

Advantages:

- Resistance to Correlation Attack and Background Knowledge Attack.

- Supporting multiuser scenario.

- High accuracy -NN search results.

Related Work:

A. Space-Filling Curves:

Space filling curves 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, .Fig. illustrate the Hilbert curves of the first three orders, where the -th order Hilbert curve can be traversed than or equal to one.

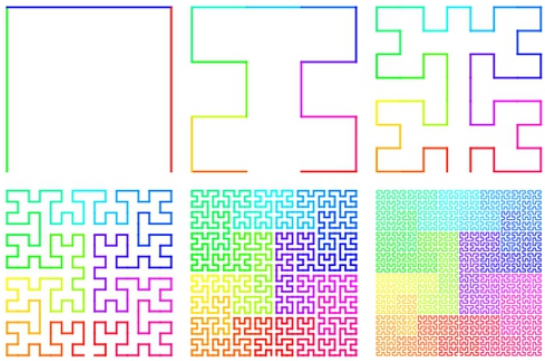


Fig. Moore curve

1) Deviations of Hilbert Curves:

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.is one of the Hilbert curve's variations and is approved in our protocol because of its end-point-connected property.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

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 an substantial constituent 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. -NN Search on Space-Filling Curves:

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

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 -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.

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 or NTRU cryptosystem, the later one even supports Homomorphic Multiplication of two ciphertexts.

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 connect the two ending points of the corresponding Moore curve.

SYSTEM MODULES:

Create System model The system model consists of three types of entities the set of users1 who wish to access location data U, a mobile service provider SP, and a location server LS. From the point of view of a user, the SP and LS will compose a server, which will serve both functions.

The user does not need to be concerned with the specific of the communication. The users in our model use some location-based service provided by the location server LS. For example, what is the nearest ATM or restaurant. The purpose of the mobile service provider SP is to establish and maintain the communication between the location server and the user.

The location server LS owns a set of POI records ri for 1 ≤ ri ≤ ρ. Each record describes a POI, giving GPS coordinates to its location (xgps,ygps), and a description or name about what is at the location. We reasonably assume that the mobile service provider SP is a passive entity and is not allowed to collude with the LS.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

We make this assumption because the SP can determine the whereabouts of a mobile device, which, if allowed to collude with the LS, completely subverts any method for privacy. There is simply no technological method for preventing this attack. As a consequence of this assumption, the user is able to either use GPS (Global Positioning System) or the mobile service provider to acquire his/her coordinates.

Initialisation:

A user u from the set of users U initiates the protocol process by deciding a suitable square cloaking region CR, which contains his/her location. All user queries will be with respect to this cloaking region. The user also decides on the accuracy of this cloaking region by how many cells are contained within it, whose size cannot be smaller than the minimum size defined by the location server.

Which is at least the minimum size defined by the server. This information is combined with the dimensions of the CR to form the public grid P and submitted to the location server, which partitions its records or superimposes it over pre-partitioned records.

This partition is denoted Q (note that the cells don't necessarily need to be the same size as the cells of P). Each cell in the partition Q must have the same number rmax of POI records. Any variation in this number could lead to theserver identifying the user.

If this constraint cannot be satisfied, then dummy records can be used to make sure each cell has the same amount of data. We assume that the LS does not populate the private grid with misleading or incorrect data, since such action would result in the loss of business under a payment model.

Transfer Phase:

The purpose of this protocol is for the user to obtain one and only one record from the cell in the public grid P. The public grid P, known by both parties, has m columns and n rows. Each cell in P contains a symmetric key ki,j and a cell id in grid Q or (IDQi,j, ki,j), which can be represented by a stream of bits Xi,j . The user determines his/her i, j coordinates in the public grid which is used to acquire the data from the cell within the grid.

We remark that this key structure of this form is an enhancement from, as the client doesn't have access to the individual components of the key.

Private Information Retrieval Phase:

With the knowledge about which cells are contained in the private grid, and the knowledge of the key that encrypts the data in the cell, the user can initiate a private information retrieval protocol with the location server to acquire the encrypted POI data.

Assuming the server has initialised the integer e, the user ui and LS can engage in the following private information retrieval protocol using the IDQi,j , obtained from the execution of the previous protocol, as input. The IDQi,j allows the user to choose the associated prime number power πi, which in turn allows the user to query the server.

Secret circular shift:

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 POIs neighbor to each other in the 2-D space. Following the same inference, the first and the last rows of H-table could be thought of as linking 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 entry (including both the first and the last one) has a neighboring relationship between its two adjacent entries. Now, if circularly shift the POI-info column of H-table two units downward but keep the H-index column intact and then make a k-NN query at Q.

In general, if want to get the same k-NN query results after shifting the POI-info column units downward circularly, just need to change our querying H-index, H-index (Q), to shifted querying H-index, shifted-H-index (Q), as shifted-H-index (Q) = H-index (Q) + (d * t) 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Algorithms Used:

Algorithms used for Privacy Preserving Location-Based Service Protocol with Secret Circular Shift are as follows

- Heuristic Cross-Like -NN Search Algorithm .
- Modified Paillier cryptosystem.

Algorithm 1:

Heuristic Cross-Like -NN Search Algorithm

Step 1:

k-Adaptive Search Window: define a –adaptive search window of size (2*D+1)2, where is the distance between the querying (or center) cell and the nearest cell on the borders of the search window. Thus, for applying PCQP to k-NN search, is chosen to be the minimum positive integer satisfying:

(2*D+1)2 ≥ k

Step 2:

Connected-Path Based k-NN Search: Within a k-adaptive search window, the Moore curve is divided into many disjoint connected paths. And based on the basic search process, the returned POIs from a k-NN search consist a connected path on the Moore curve.

Step 3:

For finding the best neighbors which are covered by a k-adaptive search window, issue k-NN queries at each connected path to achieve the full coverage.

Algorithm 2:

Modified Paillier cryptosystem

Step 1:

Key Generation: The key is generated using the following RSA modulus.

- n = pq, the RSA modulus
- λ = lcm (p − 1, q − 1)
- gEZ/(n^2 Z)×s.t g^λ=1+n mod n^2
- Public-key: (n, g), Secret key: λ

Step 2:

Encryption: The message is encrypted using the following steps.

- m E {o, 1, ..., n − 1}, a message
- h EZ/nZ
- c = gmhn mod n2, a ciphertext.

Step 3:

Decryption: The message is decrypted using the following step. m = L(cλ mod n2)

Conclusions:

In this work, a Private Circular Query Protocol with cross like search mechanism is proposed to simultaneously accomplish the location-based k-NN query and the location privacy preservation, in a novel way. To the best of our knowledge, this is the first work to apply Moore curves to location-based query problem. The proposed circular structure seamlessly integrates the robustness of specific public-key cryptosystems and the clustering property of space-filling curves. In other words, it has achieved a novel computing scheme for conducting secret computation with well-clustering property.

Expect the proposed framework not only can address the challenges of privacy preserving LBS, but also inspire the research of secret computation with desired property to achieve privacy preserving information processing. It address the problem of preserving the location privacy and user anonymity when receiving authenticated location-based services. Develop a privacy-preserving communication protocol used M-paillier cryptosystem that allows users to place queries to a location based server without revealing their identity, or current location beyond a certain accuracy.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

References:

[1]I.-Ting Lien, Yu-Hsun Lin,, Jyh-Ren Shieh, and Ja-Ling Wu, "A Novel Privacy Preserving Location-Based Service Protocol With Secret Circular Shift for -NN Search", IEEE Transactions O n Information Forensics And Security, Vol. 8, No. 6, June 2013 .

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

[3]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 and Services, 2003, pp. 31–42.

[4]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.

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

[6]A. Khoshgozaran and C. Shahabi, "Blind evaluation o f nearest Neighbor queries using space transformation to preserve location privacy," in Proc. 10th Int. Conf. Advances in Spec ial and Temporal Databases (SSTD'07), 2007, pp. 239–257.

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

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

[9]B. 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.

[10]A. 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.

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

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

[13]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.

[14]T. Onodera and K. Tanaka, "Shuffle for paillier's e ncryption scheme," IEICE Trans. Fund. Electron., Commun., Computer Sci., vol. E88-A, pp. 1241–1248, 2005

[15]D. Kahn, The Code Breakers—The Story of Secret Writing . New York, NY, USA: Macmillan, 1967.