AN IMPLEMENTABLE ENCRYPTION SOLUTION UTILIZING ACQUIRING PARITY THROUGH DISTURBANCE

[1] Dr. A. Laxmikanth,[2] M.Harshitha,[3] M.Dheeravani,[4] P.Sai Sirija,[5] K.Varasharan Kumar
[1] Professor,[2345]B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

To protect Cyber security and privacy, it is critical to design security and practical public key encryption schemes. Today, big data and cloud computing bring not only unprecedented opportunities but also fundamental security challenges, big data faces many security risks in the collection, storage and use of data and bring serious problem regarding the disclosure of private user data. It is challenging to achieve security and privacy protection in the big data environment.

Thus, to meet the growing demand of public key encryption in this environment, we proposed a single-bit public key encryption schemes based on a variant of LPN (Learning Parity with Noise) and extended it to a multi-bit public key encryption scheme. We provide the correctness and CPA (Chosen Plain Attack) security of the proposed method. Our schemes solved encoding error rate problem of the existing public key schemes based on LPN, and the error rate in our schemes in negligible.

I. INTRODUCTION

Big data faces many security risks in the collection, storage and use of data and brings serious problems regarding the disclosure of private user data. Thus, to meet the growing demand of public key encryption in this environment, we proposed a single- bit public key encryption scheme based on a variant of LPN (Learning Parity with Noise) and extended it to a multi-bit public key encryption scheme. We proved the correctness and CPA (Chosen Plaintext Attack) security of the proposed method. With the development and application of big data and cloud computing technology, the large data environment has put forward higher requirements for data encryption, and the design of a practical and secure public key encryption scheme has important practical significance. Considering data security in the big data environment, many valuable schemes have been put forward.

They have been shown to be useful in applications such as protecting the privacy in machine learning and protecting security in cloud computing. The main classical public key schemes were designed based on a number of difficult number theory problems, such as large number factorization and discrete logarithms. However, many traditional number theory assumptions on which the above schemes are based can be solved by quantum algorithms. That is, in the era of quantum computing, these public key encryption schemes have been broken. Therefore, in the post quantum era, new public key encryption schemes based on new difficult problems need to be designed and 2169-3536 (c) 2018 IEEE.

Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. Implemented for the new computing environments and applications. In 2003, Boneh and Silverberg defined the concept of ideal multilinear mapping and demonstrated its application scenarios. However, until 2013, Garg, Gentry and Halevi (GGH) proposed the first realistic multilinear mapping based on ideal lattice [16], with its security based on the multi-level Diffie-Hellman computation and decision problem (GCDH/GDDH). Many new schemes have been designed based on the GGH scheme. Recently, the GGH scheme was proved to be insecure, and new multilinear mapping construction is being explored. Regev proposed LWE (Learning with Error) based on lattice theory, which has been widely used in public key cryptosystem design and applications of data encryption.

II. LITERATURE SURVEY

1. TITLE: CCA Secure Public Key Encryption Scheme Based on LWE Without Gaussian Sampling.

AUTHOR: Xiaochao Sun, Bao Li, Xianhui Lu, Fuyang Fang.

ABSTRACT: We present a CCA secure PKE

based on the problem of the LWE with uniform errors. We use one of the instantiations of parameters of LWE with uniform errors suggested by Micciancio and Peikert (CRYPTO 2013). Since the uniform errors do not bear the Fourier-properities as the Gaussian errors, the statistical techniques and tools used b Micciancio and Peikert (EUROCRYPT 2012) to construct errors. However, we conquer the problem by employing the double-trapdoor mechanism to construct a tag-based encryption with CCA security and transform it ti a CCA secure PKE from the generic conversion based on one-time signatures.

2. TITLE: Dynamic Fully Homomorphic Encryption-based Merkle Tree for Lightweight Streaming Authenticated Data Structures.

AUTHOR: Jian Xu, Laiwen Wei, Yu Zhang, Andi Wang, Fucai Zhou, and Chong-zhi. ABSTRACT: Fully Homomorphic encryption-based Merkle Tree (FHMT) is a novel technique for streaming authenticated data structures (SADS) to achieve the streaming verifiable computation. By leveraging the computing capability of fully homomorphic encryption, FHMT shifts almost all of the computation tasks to the server, reaching nearly no overhead for the client. Therefore, FHMTis an important technique to construct a more efficient lightweight ADS for resource-limited clients. But the typical FHMT cannot support the dynamic scenario very well because it cannot expend freely since its height is fixed. We now present our fully dynamic FHMT construction, Which is a construction that is able to authenticate an unbounded number of data elements and improves upon the state-of-the-art in terms of computational overhead. We divided the algorithms of the DFHMT with the following phases: initialization, insertion, tree expansion, query and verification. The DFHMT removes the drawbacks of the static FHMT. In the initialization phase, it is not required for the scale of the tree to be determined, and the scale of the tree can be adaptively expanded during the data- appending phase. This feature is more suitable for streaming data environments. We analyzed the securityof the DFHMT, and point out that DFHMT has the same security with FHMT. The storage, communication and computation overhead of DFHMT is also analyzed, the results show that the client uses simple numerical multiplications and additions to replace hash operations, which reduces the computational burden of the client; the length of the authentication path in DFHMT is Shorter than FHMT, which reduces storage and communication overhead. The performance of DFHMT was compared with other construction techniques of SADS via some tests, the results show that DFHMT strikes the performance balance between the client and server, which has some performance advantage for lightweight devices.

3. TITLE: DivORAM:Towards a Practical Oblivious RAM with Variable Block Size.

AUTHOR: Zheli Liu, Yanyu Huang, Jin Li, Xiaochun Cheng, and Chao Shen. ABSTRACT: Oblivious RAM (ORAM) is important for applications that require hiding access patterns. Many ORAM schemes have been proposed but most of them support only storing blocks of the same size. For the variable length data blocks, they usually fill them upto the same length before uploading, which leads to an increase in storage space and network bandwidth usage. To develop the first practical ORAM with variable block size, we proposed the “DivORAM” by remodeling the tree- based ORAM structure. It employs an additively homomorphic encryption scheme (Damgård–Jurik cryptosystem) executing at the server side to save the client computing overhead and the network bandwidth cost. As a result, it saves network bandwidth 30% comparing withRing ORAM and 40% comparing with HIRB ORAM. Experiment results show that the response time of DivORAM is 10× improved over Ring ORAM for practical parameters.

4. TITLE: Differentially Private Naive Bayes Learning over Multiple Data Sources.

AUTHOR: Tong Li, Jin Li, Zheli Liu, Ping Li, and Chunfu Jia.

ABSTRACT: For meeting diverse requirements of data analysis, the machine learning classifier has been provided as a tool to evaluate data in many applications. Due to privacy concerns of preventing disclosing sensitive information, data owners often suppress their data for an untrusted trainer to train a classifier. Some existing work proposed privacy-preserving solutions for learning algorithms, which allow a trainer to build a classifier over the data from a single owner.

However, they cannot be directly used in the multi-owner setting where each owner is not totally trusted for each other. In this paper, we propose a novel privacy-preserving Naive Bayes learning scheme with multiple data sources. The proposed scheme enables a trainer to train a Naive Bayes classifier-over the dataset provided jointly by different data owners, without the help of a trusted curator. The training result can achieve ϵ-differential privacy while the training will not break the privacy of each owner. We implement the prototype of the scheme and conduct corresponding experiment.

5. TITLE:Privacy-Preserving Naive Bayes Classifiers Secure against the Substitution-then- Comparison Attack.

AUTHOR: Chong-Zhi Gao, Qiong Cheng, Pei He, Willy Susilo, and Jin Li

ABSTRACT: Naive Bayes (NB) is a simple but highly practical classifier, with a wide range of applications including spam filters, cancer diagnosis and face recognition, to name a few examples only. Consider a situation where a user requests a classification service from a NB classifier server, both the user and the server do not want to reveal their private data to each other. This paper focuses on constructing a privacy-preserving NB classifier that is resistant to an easy-to-perform, but difficult- to-detect attack, which we call the substitution-then-comparison (STC) attack. Without resorting to fully homomorphic encryptions, which has a high computational overhead, we propose a scheme which avoids information leakage under the STC attack. Our key technique involves the use of a "double-blinding" technique, and we show how to combine it with additively homomorphic encryptions and oblivious transfer to hide both parties' privacy. Furthermore, a completed evaluation shows that the construction is highly practical - most of the computations are in the server's offline phase, and the overhead of online computation.

6. TITLE: Identity-based Encryption with Outsourced Revocation in Cloud Computing.

AUTHOR: Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, Wenjing Lou.

ABSTRACT: Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this paper, aiming at tackling the critical issue of identity revocation.we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally. This goal is achieved by utilizing a novel collusion-resistant technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore, we propose another construction which is provable secure under the recently formalized Refereed Delegation of Computation model.

7. TITLE: Multi-keyprivacy-preserving deep learning in cloud computing.

AUTHOR: Ping Li, J in Li, Zhengan Huang, TongLi, Chong-Zhi Gao, Siu-Ming.

ABSTRACT: Deep learning has attracted a lot of attention and has been applied successfully in manyareas such as bioinformatics, imaging processing, game playing and computer security etc. On the other hand, deep learning usually requires a lot of training data which may not be provided by a sole owner. As the volume of data gets huge, it is common for users to store their data in a third-party cloud. Due to the confidentiality of the data, data are usually stored in encrypted form. To apply deep learning to these datasets owned by multiple data owners on cloud, we need to tackle two challenges: (i) the data are encrypted with different keys, all operations including intermediate results must be secure; and (ii) the computational cost and the communication cost of the data owner(s) should be kept minimal. In our work, we propose two schemes to solve the above problems. We first present a basic scheme based on multi-key fully homomorphic encryption (MK-FHE), then we propose an advanced scheme based

on a hybrid structure by combining the double decryption mechanism.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

The existing scheme is still having the problem of decryption error, which is not satisfactory. Based on the LPN variants problem, we proposed a single-bit and a multi-bit public key encryption scheme. Our scheme solved the decryption error problem of the existing public key encryption schemes based on DLPN. Big data faces many security risks in the collection, storage and use of data and brings serious problems regarding the disclosure of private user data.

Disadvantages of Existing System:

- The existing scheme is still having the problem of decryption error, which is not satisfactory.
- Big data faces many security risks in the collection, storage and use of data and brings serious problems regarding the disclosure of private user data.

1.2 PROPOSED SYSTEM:

We proposed a single-bit public key encryption scheme based on a variant of LPN (Learning Parity with Noise) and extended it to a multi-bit public key encryption scheme. We proved the correctness and CPA (Chosen Plaintext Attack) security of the proposed method. Our schemes solved encoding error rate problems of the existing public key schemes based on LPN, and the encoding error rate in our schemes is negligible.

Advantages of Proposed System:

- We maintain the largest advantages of LPN, which are rapid instance generation, and rapid and efficient encryption and decryption computing.
- We solve the encoding error problem of existing public key encryption schemes

SYSTEM ARCHITECTURE

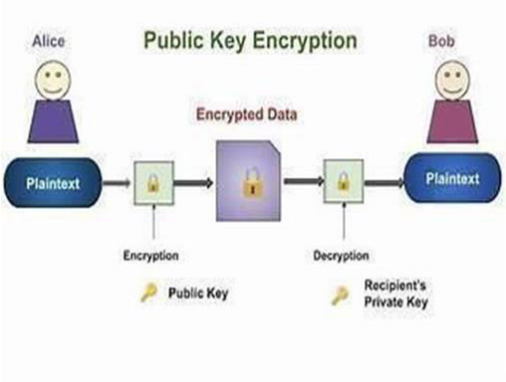


Fig. SYSTEM ARCHITECTURE

IV. IMPLEMENTATION

MODULES

- USER
- ADMIN

MODULE DESCRIPTION

User

In this project user Is one of the module here user should register with the application and the user authorized by the admin then only the user can able login into the application the user can view his profile, can create or sends the message to other user who are already registered with our application and the user can generate the decryption key to view the message by the requested user, and also the user block the another users also because if that user send any noise information.

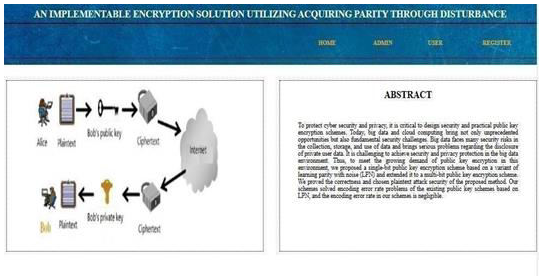
Admin

The admin is the main module in this project, the admin can login directly without login with the application and the admin should authorize the users, and can add the noise words, can check the blocked user details and also check the encryption and decryption time of the message communicated between two users.

V. SCREENSHOTS:

User login screenshots

A login screen is a user interface that is displayed when a user is required to enter their login credentials to access a system or service. User-Login means a unique username and associated password provisioned to an identifiable individual to permit them to access the Services.

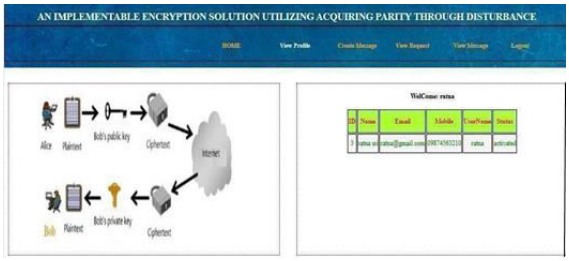


Figno. 1 Home Page

Fig no.2 Register Page

Fig no.3 User Login Page

Figno.4Welcome User Page



Figno.5View Profile Page

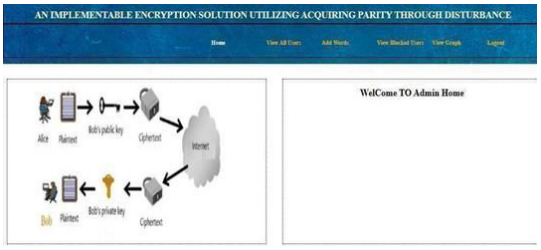
Figno.6 Create Message Page

Figno.7 View Request page

Figno.8 View Message Page

Admin Login Screenshots

A login screen is a user interface that is displayed when a user is required to enter their login credentials to access a system or service. Login or entry available to the user of a discussion forum or website with special rights to control or restrict the activity of other users.



Figno.9 Admin Home Page

Figno.10 View All Users

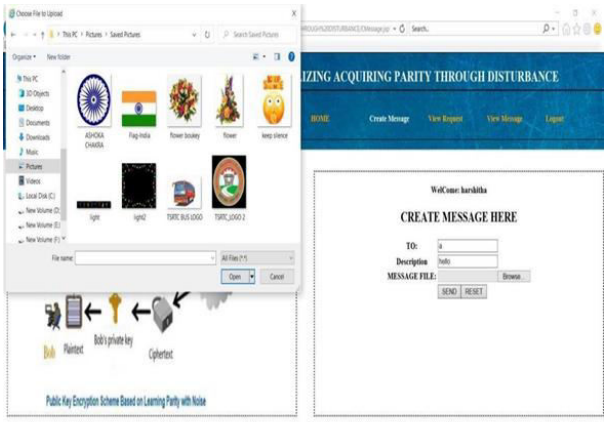
Figno.11 Add Words Page

Figno.12 View Blocked Users

Figno.13 View Graph Page

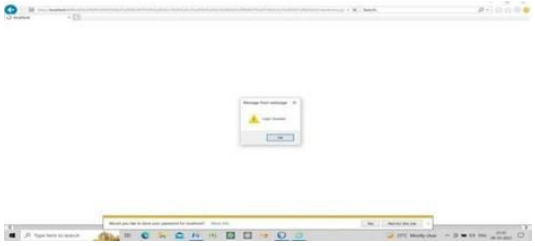
Webcam Application

A webcam is a video camera that is connected to a computer or other device, typically via USB port, and is used to capture and transmit video over the internet. Webcams are commonly used for videoconferencing, live streaming, and other applications that require real-time video communication.

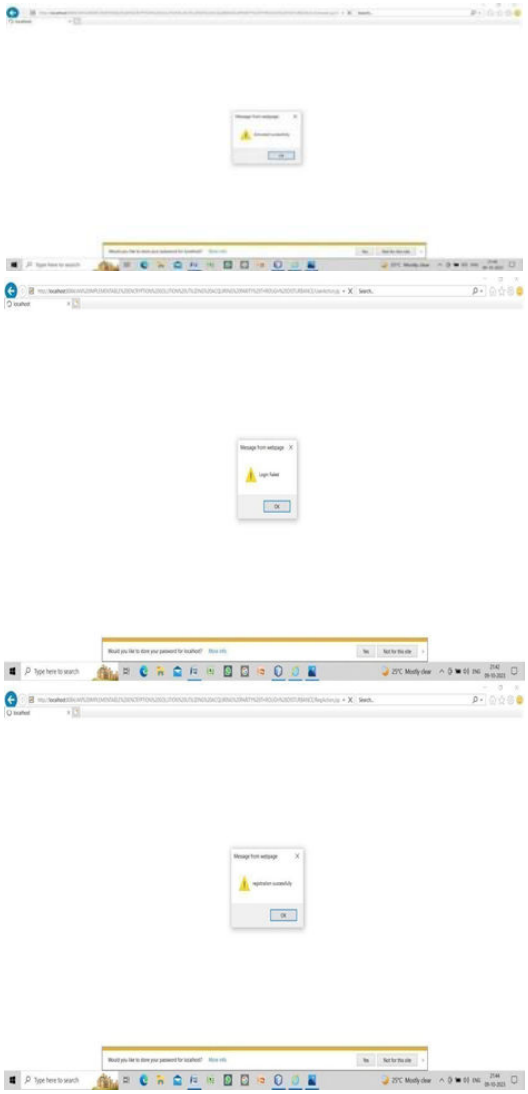


Alert Messages

Alert messaging (or alert notification) is machine-to-person communication that is important or time-sensitive. An alert may be a calendar reminder or a notification of a new message.



Figno. 10.2.15 Alert messages pages



VI. CONCLUSION

CONCLUSION

In the post quantum era, the design of public key cryptography under the DLPN assumption is an important research direction. Such schemes have many advantages such as shorter public key and cipher text, faster encryption and decryption. But the existing scheme is still having the problem of decryption error, which is not satisfactory. Based on the LPN variants problem, we proposed a single- bit and a multi-bit public key

Encryption scheme. Our scheme solved the decryption error problem of the existing public key encryption schemes based on DLPN. Compared to existing schemes, there is an increase in only a small amount of cipher text space and computing overhead in our scheme. Our scheme not only is able to withstand quantum attack but also provides strong practical security at the same time. In the

future, we will design a public key scheme based DLPN with high security, smaller public key and cipher text size, and smaller computational overhead. Furthermore, designing public key cryptography that satisfies CCA security is also one of our future works.

FUTURE SCOPE

Safeguarding user information in contextual social networks is a critical concern given the increasing amount of personal data shared and the potential privacy risks associated with it. Here are some future-focused strategies and considerations for enhancing user information protection in contextual social networks:

1. Privacy by Design and Default:

Implementing privacy features in to the design and architecture of social networks from the outset. Privacy should be the default setting, and users should have granular control over their data sharing preferences.

2. Advanced Encryption and Security Measures

Enhancing encryption protocol sand adopting state-of-the-art security measures to protect user data both during storage and transmission within the social network platform.

3. Decentralized Identity and Authentication:

Implementing decentralized identity systems, like blockchain- based solutions, to allow users to control and manage their identity and personal data independently from the social network. Enhancing privacy and security.

Collaboration and Information Sharing: Encouraging collaboration and sharing of best practices within the industry to collectively work towards developing more secure and privacy-focused solutions for contextual social networks the future of safeguarding user information in contextual social networks will involve a multidimensional approach, incorporating technology advancements, regulatory compliance, user empowerment, and a commitment to respecting individual privacy. Balancing the benefits of data sharing with the imperative to protect user privacy will be a central challenge in the evolving landscape of social networking.

REFERENCES

1. R. Agrawal, A. Evfimievski, and R. Srikant, Information sharing across private databases, in SIGMOD 2003, pp. 86-97.
2. M. von Arb, M. Bader, M. Kuhn, and R. Watten hofer, Veneta: Server less friend-of-friend detection in mobile social networking, in IEEE WIMOB 2008, pp. 184-189.
3. B.H. Bloom, Space/time trade-offs in hash coding with allowable errors, Communications of the ACM 13 (7): 422-426, 1970.
4. D.Bonch,E.J.Goh,K.Nissim,Evaluating2-DNFformulason ciphertexts, in TCC2006, pp 325- 341.
5. D. Chaum, Blind signatures for untrace able payments, in Crypto 1982, pp. 199-203.
6. E.D.Cristofaro and G. Tsudik, Practical private set intersection protocols with linear complexity, in Financial Cryptography and Data Security 2010.
7. D. Dachman -Soled. T. Malkin, M. Raykova, and M.Yung. Efficient robust private set intersection, in ACNS 2009, pp. 125-142.
8. T.ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (4): 469-472, 1985.
9. M.Freedman, K. Nissim, and B. Pinkas, Efficient private matching and set intersection, in EUROCRYPT 2004, pp. 1-19.
10. C. Gentry, Fully homomorphic encryption using ideal lattices, in STOC 2009, pp 169-178.
11. Zhe Liu, Le Yu, Wenbo He, “Privacy and Security in Online Social Networks : A Survey” Published in : IEEE Communications Surveys & Tutorials, 2015.
12. Joseph Bonneau, Sören Preibusch,“A Survey of Privacy in Online Social Networks Published in: ACM Computing Surveys, 2010.
13. Wenjia Li, Lingling Xu, et al.. “Privacy-Preserving Location- Based Services for Mobile Users in Cloud Computing ” Published in: IEEE Transactions on Emerging Topics in Computing, 2015.
14. ShoulingJi,etal.,“Securing the Privacy of Sensitive User Profile Attributes in Social Networks” Published in: IEEE Transactions

on Information Forensics and Security, 2013.

15. Petra M.Mäntylä,TarmoToikkanen, “Building Online Communities in Higher Education Institutions:Creating Collaborative Experience” Published in: pringer, 2018.