International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 3 300 – 303

Enhanced Searchable Public Key Cipher Text With Hidden Structures For Fast Keyword Search

Avhad Shivaji A.
B.E Computer
BVCOERI,Nashik
saavhad22@gmail.com

Varade Jyoti K.
B.E Computer
BVCOERI,Nashik
jyotikvarade@gmail.com

Aulagar Naveen S.
B.E Computer
BVCOERI,Nashik
naveen4181@live.com

Prof. S.A. Handore
Project Guide
BVCOERI,Nashik
sonali.handore@engg.brahmavalley.com

Abstract - Existing semantically secure public-key searchable coding schemes take search time linear with the overall variety of the cipher texts. This makes retrieval from large-scale databases preventative. To alleviate this drawback, this paper proposes Searchable Public-Key Cipher texts with Hidden Structures (SPCHS) for keyword search as quick as potential while not sacrificing linguistics security of the encrypted keywords. In SPCHS, all keyword-searchable Cipher texts area unit structured by hidden relations, and with the search trapdoor such as a keyword, the minimum info of the relations is disclosed to an enquiry rule because the steering to search out all matching Cipher texts expeditiously. We have a tendency to construct a SPCHS theme from scratch during which the Cipher texts have a hidden star-like structure. We have a tendency to prove our theme to be semantically secure within the Random Oracle (RO) model. The search quality of our theme relies on the particular variety of the Cipher texts containing the queried keyword, instead of the amount of all Cipher texts. Finally, we have a tendency to gift a generic SPCHS construction from anonymous identity-based coding and collision-free full-identity malleable Identity-Based Key Encapsulation Mechanism (IBKEM) with namelessness. We have a tendency to illustrate 2 collision-free full-identity malleable IBKEM instances, that area unit semantically secure and anonymous, severally, within the artificial language and customary models.

Keywords - *Public-Key, Cipher texts, IBKEM,RSA*

*****

1. INTRODUCTION

PUBLIC-KEY coding with keyword search (PEKS), introduced by Boneh et al. in , has the advantage that anyone UN agency is aware of the receiver's public key will transfer keyword-searchable Cipher texts to a server. additional specifically, every sender individually encrypts a file and its extracted keywords and sends the ensuing Cipher texts to a server; once the receiver desires to retrieve the files containing a selected keyword, he delegates a keyword search trapdoor to the server; the server finds the encrypted files containing the queried keyword while not knowing the first files or the keyword itself, and returns the corresponding encrypted files to the receiver; finally, the receiver decrypts these encrypted files1. The authors of PEKS [1] additionally bestowed linguistics security against chosen keyword attacks (SSCKA) within the sense that the server cannot distinguish the Cipher texts of the keywords of its selection before observant the corresponding keyword search trapdoors. It appears Associate in nursing applicable security notion, particularly if the keyword area has no high min-entropy. Existing semantically secure PEKS schemes take search time linear with the entire variety of all Cipher texts. This makes retrieval from large-scale databases preventive. Therefore, additional economical search performance is crucial for much deploying PEKS schemes. one among the outstanding works to accelerate the search over encrypted keywords within the public-key setting is settled coding introduced by Bellare et al. in Associate in Nursing coding theme is settled if the coding rule is settled. Bellare et al [2] target sanctioning search over encrypted keywords to be as economical as the explore for unencrypted keywords, such a cipher text containing a given keyword will be retrieved in time complexness power within the total variety of all Cipher texts. {this is this is often this will be} cheap as a result of the encrypted keywords can type a tree-like structure once keep in step with their binary values. However, settled coding has 2 inherent limitations. First, keyword privacy will be secure just for keywords that ar a priori hardto- guess by the antagonist (i.e., keywords with high minentropy to the adversary); second, sure info of a message leaks inevitably via the ciphertext of the keywords since the coding is settled. Hence, settled coding is simply applicable in special eventualities.

2. LITERATURE SURVEY

Boneh D., Crescenzo G. D., Ostrovsky R., Persiano G [1] stated problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email

gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

Bellare M., Boldyreva A., O'Neill A [2] present as-strong-as-possible definitions of privacy, and constructions achieving them, for public-key encryption schemes where the encryption algorithm is deterministic. We obtain as a consequence database encryption methods that permit fast (i.e. sub-linear, and in fact logarithmic, time) search while provably providing privacy that is as strong as possible subject to this fast search constraint. One of our constructs, called RSA-DOAEP, has the added feature of being length preserving, so that it is the first example of a public-key cipher. We generalize this to obtain a notion of efficiently-searchable encryption schemes which permit more flexible privacy to search-time trade-offs via a technique called bucketization. Our results answer much-asked questions in the database community and provide foundations for work done there.

Boneh D., Boyen X .[3] construct two efficient Identity Based Encryption (IBE) systems that are selective identity secure without the random oracle model. Selective identity secure IBE is a slightly weaker security model than the standard security model for IBE. In this model the adversary must commit ahead of time to the identity that it intends to attack, whereas in the standard model the adversary is allowed to choose this identity adaptively. Our first secure IBE system extends to give a selective identity Hierarchical IBE secure without random oracles.

Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles) by Boyen X., Waters B. R. [4], they present an identity-based cryptosystem that features fully anonymous Cipher texts and hierarchical key delegation. We give a proof of security in the standard model, based on the mild Decision Linear complexity assumption in bilinear groups. The system is efficient and practical, with small Cipher texts of size linear in the depth of the hierarchy. Applications include search on encrypted data, fully private communication, etc. The system resolve two open problems pertaining to anonymous identity-based encryption, our scheme being the first to offer provable anonymity in the standard model, in addition to being the first to realize fully anonymous HIBE at all levels in the hierarchy.

According to Gentry C [5] Practical Identity-Based Encryption Without Random Oracles present an Identity Based Encryption (IBE) system that is fully secure in the standard model and has several advantages over previous such systems – namely, computational efficiency, shorter public parameters, and a "tight" security reduction, albeit to a stronger assumption that depends on the number of private key generation queries made by the adversary. Our assumption is a variant of Boneh et al.'s decisional Bilinear Diffie-Hellman Exponent assumption, which has been used to construct efficient hierarchical IBE and broadcast encryption systems. The construction is remarkably simple. It also provides recipient anonymity automatically, providing a second (and more efficient) solution to the problem of achieving anonymous IBE without random oracles. Finally, our proof of CCA2 security, which has more in common with the security proof for the Cramer-Shoup encryption scheme than with security proofs for other IBE systems, may be of independent interest.

3. EXISTING SYSTEM:

One of the outstanding works to accelerate the search over encrypted keywords within the public-key setting is settled cryptography introduced by Bellare et al. Associate in Nursing cryptography theme is settled if the cryptography algorithmic rule is settled. Bellare et al. concentrate on facultative search over encrypted keywords to be as economical because the look for unencrypted keywords, such a ciphertext containing a given keyword are often retrieved in time complexness power within the total variety of all Cipher texts. this is often be} cheap as a result of the encrypted keywords can kind a tree-like structure once keep per their binary values. Search on encrypted information has been extensively investigated in recent years. From a cryptographical perspective, the prevailing works constitute 2 classes, i.e., bilaterally symmetrical searchable cryptography and public-key searchable cryptography.

2.1 Disadvantages of Existing System:

Existing semantically secure PEKS schemes take search time linear with the total number of all cipher texts. This makes retrieval from large-scale databases prohibitive. Therefore, more efficient search performance is crucial for practically deploying PEKS schemes.

Deterministic encryption has two inherent limitations. First, keyword privacy can be guaranteed only for keywords that are a priori hard to guess by the adversary (i.e., keywords with high min-entropy to the adversary); second, certain information of a message leaks inevitably via the ciphertext

of the keywords since the encryption is deterministic. Hence, deterministic encryption is only applicable in special scenarios. The linear search complexity of existing schemes is the major obstacle to their adoption.

4. PROPOSED SYSTEM:

We are interested in providing highly efficient search performance without sacrificing semantic security in PEKS. We start by formally defining the concept of Searchable Public-key Cipher texts with Hidden Structures (SPCHS) and its semantic security. In this new concept, keyword searchable Cipher texts with their hidden structures can be generated in the public key setting; with a keyword search trapdoor, partial relations can be disclosed to guide the discovery of all matching Cipher texts. Semantic security is defined for both the keywords and the hidden structures. It is worth noting that this new concept and its semantic security are suitable for keyword-searchable Cipher texts with any kind of hidden structures. In contrast, the concept of traditional PEKS does not contain any hidden structure among the PEKS Cipher texts; correspondingly, its semantic security is only defined for the keywords.

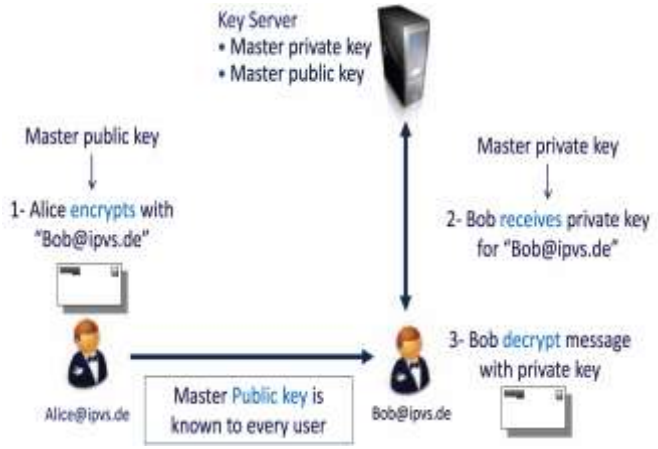

Fig.1. System Architecture

4.1 Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

4.2 Objectives

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

4.3 Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

5. MODULE DESCRIPTION

5.1 Data owner Module

Searchable Public-Key Cipher texts with Hidden Structures (SPCHS) for keyword search as fast as possible without sacrificing semantic security of the encrypted keywords. In SPCHS, all keyword-searchable Cipher texts are structured by hidden relations, and with the search trapdoor corresponding to a keyword, the minimum information of the relations is disclosed to a search algorithm as the guidance to find all matching Cipher texts efficiently

5.2 Data User Module

In this module, we develop the data user module. It start by formally defining the concept of Searchable Public-key Cipher texts with Hidden Structures (SPCHS) and its semantic security. In this new concept, keyword searchable cipher texts with their hidden structures can be generated in the public key setting; with a keyword search trapdoor, partial relations can be disclosed to guide the discovery of all matching cipher texts.

5.3 Encryption Module

Anonymous identity-based broadcast encryption. A slightly more complicated application is anonymous identity-based broadcast encryption with efficient decryption. An analogous application was proposed respectively by Barth et al. and Libert et al. in the traditional public-key setting. With collision-free fullidentity malleable IBKEM, a sender generates an identity based broadcast ciphertext hC1, C2, (K1 1 jjSE(K1 2 ; F1)), :::, (KN 1 jjSE(KN 2 ; FN))i, where C1 and C2 are two IBKEM encapsulations,

5.4 Rank Search Module

It allows the search to be processed in logarithmic time, although the keyword search trapdoor has length linear with the size of the database. In addition to the above efforts devoted to either provable security or better search performance

6. CONCLUSION

This paper investigated as-fast-as-possible search in PEKS with semantic security. This concept of SPCHS as a variant of PEKS. The new concept allows keyword-searchable Cipher texts to be generated with a hidden structure. Given a keyword search trapdoor, the search algorithm of SPCHS can disclose part of this hidden structure for guidance on finding out the Cipher texts of the queried keyword. Semantic security of SPCHS captures the privacy of the keywords and the invisibility of the hidden structures. An SPCHS scheme from scratch with semantic security in the RO model of proposed system. The scheme generates keyword-searchable Cipher texts with a hidden star-like structure. It has search complexity mainly linear with the exact number of the Cipher texts containing the queried keyword. It outperforms existing PEKS schemes with semantic security, whose search complexity is linear with the number of all Cipher texts. We identified several interesting properties, i.e., collision-freeness and full-identity malleability in some IBKEM instances, and formalized these properties to build a generic SPCHS construction. We illustrated two collision-free full-identity malleable IBKEM instances, which are respectively secure in the RO and standard models.

REFERENCES

[1] Boneh D., Crescenzo G. D., Ostrovsky R., Persiano G.: Public Key Encryption with Keyword Search. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506-522. Springer, Heidelberg (2004)

[2] Bellare M., Boldyreva A., O'Neill A.: Deterministic and Efficiently Searchable Encryption. In: Menezes A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 535-552. Springer, Heidelberg (2007)

[3] Boneh D., Boyen X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223-238. Springer, Heidelberg (2004)

[4] Boyen X., Waters B. R.: Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In: Dwork C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290-307. Springer, Heidelberg (2006)

[5] Gentry C.: Practical Identity-Based Encyrption Without Random Oracles. In: Vaudenay S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp.445-464. Springer, Heidelberg (2006)