Fast Keyword Search Using Public-Key Ciphertexts With Hidden Structures

K.Maheshwari[1], S. Nithya dhevi[2]

[1]PG student, Dept. of Computer Science Engineering, Sir Isaac Newton College Of Engineering technology, Pappakoil, Nagapattinam-611001, India

[2] Assistant Professor, Dept. of Computer Science Engineering , Sir Isaac Newton College Of Engineering technology, Pappakoil, Nagapattinam-611001, India

---***---

Abstract - *Searchable Public-Key Ciphertexts with Hidden Structures for keyword search is as fast as possible without sacrificing semantic security of the encrypted keywords. In SPCHS, all keyword-searchable ciphertexts 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 ciphertexts efficiently. Construct a SPCHS scheme from scratch in which the ciphertexts have a hidden star-like structure. The scheme is to be semantically secure in the Random Oracle model. The search complexity of is dependent on the actual number of the ciphertexts containing the queried keyword, rather than the number of all ciphertexts. SPCHS construct from anonymous identity-based encryption and collision-free full-identity malleable Identity-Based Key Encapsulation Mechanism with anonymity. Two collision-free full-identity malleable IBKEM instances are semantically secure and anonymous, respectively, in the RO and standard models. The latter instance enables us to construct an SPCHS scheme with semantic security in the standard model.*

Key Words: Public–key searchable encryption, Semantic security, Identity–Based Encapsulation Mechanism (IBKEM), Identity–Based Encryption (IBE).

1.INTRODUCTION

1.1 Cloud Networking

New networking paradigm is mainly for building and managing secure private networks over the public Internet by utilizing global cloud computing infrastructure. Traditional network functions and services including connectivity, security, management and control, are pushed to the cloud and delivered as a service. Two categories of cloud networking are Cloud–Enabled Networking and Cloud–Based Networking.

1.2 Public-Key Searchable Encryption

Public-Key Encryption with Keyword Search (PEKS), has the advantage that anyone who knows the receiver's public key can upload keyword-searchable ciphertexts to a server. The receiver can delegate the keyword search to the server. Each sender separately encrypts a file and its extracted keywords and sends the resulting ciphertexts to a server.

1.3 Semantic Security

Semantic security against chosen keyword attacks (SSCKA) in the sense that the server cannot distinguish the ciphertexts of the keywords of its choice before observing the corresponding keyword search trapdoors. It seems an appropriate security notion, especially if the keyword space has no high min-entropy. Improve search performance in PEKS without sacrificing semantic security if one can organize the ciphertexts with elegantly designed but hidden relations.

1.4 Overview Of The Project

Keyword searchable ciphertexts 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 ciphertexts. Semantic security is defined for both the keywords and the hidden structures. Worth noting that this new concept and its semantic security are suitable for keyword-searchable ciphertexts with any kind of hidden structures. In contrast, the concept of traditional PEKS does not contain any hidden structure among the PEKS ciphertexts. Correspondingly, its semantic security is only defined for the keywords. Following the SPCHS definition, construct a simple SPCHS from scratch in the random oracle model. The scheme generates keyword-searchable ciphertexts with a hidden star-like structure. The search performance mainly depends on the actual number of the ciphertexts containing the queried keyword. For security, the scheme is proven semantically secure based on the Decisional Bilinear Diffie Hellman (DBDH) assumption in the RO model.

A generic SPCHS construction with Identity Based Encryption (IBE) and collision-free full-identity malleable IBKEM. The resulting SPCHS can generate keyword-searchable ciphertexts with a hidden star-like structure.

Moreover, if both the underlying IBKEM and IBE have semantic security and anonymity, the resulting SPCHS is semantically secure. An SPCHS construction is reduced to collision-free full-identity malleable IBKEM with anonymity. Several IBKEM schemes are proposed to construct Verifiable Random Functions. One of these IBKEM schemes is anonymous and collision-free full identity malleable in the RO model. We transform this IBE scheme into a collision-free full-identity malleable IBKEM scheme with semantic security and anonymity in the standard model. Hence, this new IBKEM scheme allows us to build SPCHS schemes secure in the standard model with the same search performance as the previous SPCHS construction from scratch in the RO model.

2. LITERATURE SURVEY

Arriaga.A, et al. [1] proposes the notion of Strong Search Pattern Privacy for PEKS and construct a scheme that achieves this security notion. He provide a broader view on trapdoor privacy in asymmetric searchable encryption, and bridge the gap between currently existent definitions. He shows that two distinct scenarios to model trapdoor privacy one in the presence of ciphertexts that match trapdoors, and the other in the absence of such ciphertexts. The notion of Strong Search Pattern Privacy addresses privacy concerns up to the point where ciphertexts matching the issued trapdoors become available, after which, search patterns can no longer be hidden from an attacker. Remains an open problem to achieve security according to the generalized definition of Adaptive Key Unlinkability.

Ateniese.G, et al. [2] introduces UAnonIBE the first universally anonymous, thus key-private, IBE security is based on the standard quadratic residuosity assumption. The main aspect characterizing universal anonymity is the ability to separate the role of the sender of encrypted messages from the role of the anonymzer. An encryption scheme is universally anonymous if ciphertexts can be made anonymous by anyone and not just by whoever created the ciphertexts. Specifically, a universally anonymizable public-key encryption scheme consists of a standard public-key encryption scheme and two additional algorithms one is used to anonymize ciphertexts, which takes as input only the public key of the recipient, and the other is used by the recipient to decrypt anonymized ciphertexts. It is more expensive and still depending on pairing-based assumptions.

Bellare.M, et al. [3] presents as-strong-as-possible definitions of privacy, and constructions achieving them, for public-key encryption schemes where the encryption algorithm is deterministic. Obtain as a consequence database encryption methods that permit fast search while provably providing privacy that is as strong as possible subject to this fast search constraint. One of their constructs, called RSA-DOAEP, has the added feature of being length preserving, so that it is the first example of a public-key cipher. 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. Weakness of this paper is only provide privacy for plaintexts that have high min-entropy.

Boneh.D, et al. [4] proposes searching on data that is encrypted using a public key system. He 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. Proves security by exploiting extra properties. The weakness of PEKS is to remove secure channel and encrypt multiple keywords. Another problem is to refresh frequently-used keywords. Enables one to search encrypted keywords without compromising the security of the original data.

Boneh.D, et al. [5] constructs two efficient Identity Based Encryption (IBE) systems that are selective identity secure without the random oracle model in groups equipped with a bilinear map. Selective identity secure IBE is a slightly weaker security model than the standard security model for IBE. First system is based on the decisional bilinear Diffie-Hellman assumption, and extends to give a selective identity Hierarchical IBE secure without random oracles. Second system is based on a related assumption called the bilinear Diffie-Hellman inversion assumption. Observe that a selective-ID secure IBE system implies a fully secure IBE system but the resulting security reduction is not polynomial. The system is quite impractical and should only be viewed as a constructive proof that such constructions are indeed possible. The question of constructing a fully secure IBE system with a tight reduction in the standard model remains open.

Boyen.X, et al. [6] presents an identity-based cryptosystem that features fully anonymous ciphertexts and hierarchical key delegation. Novel linear-splitting technique which prevents an attacker from testing the intended recipient of ciphertexts, yet allows for the use of randomized private IBE keys. In the hierarchical case, add a new multi-simulation proof device that permits multiple HIBE subsystems to concurrently re-randomize each other. Security is based solely on the Linear assumption in bilinear groups. It is based on the mild Decision Linear complexity assumption in bilinear groups. The system is efficient and practical, with small ciphertexts of size linear in the depth of the hierarchy. Results resolve two open problems pertaining to anonymous IBE - Offer provable anonymity in the standard model and Realize fully anonymous HIBE at all levels in the hierarchy.

This paper has a drawback that is an anonymous IBE and HIBE scheme without using random oracles.

Ducas L. [7] presented a technique for using asymmetric bilinear groups to add anonymity to a family of non-anonymous HIBE systems. A HIBE system is anonymous if the ciphertext reveals no information about the public-key used to create it. An extension of IBE, called Hierarchical-IBE allows for a hierarchy of identities where any path from the root to a node can function as a public-key. An IBE or HIBE is said to be recipient anonymous or simply anonymous if the ciphertext leaks no information about the public key used to create it. Both anonymous IBE and HIBE are building blocks for encryption systems supporting searching on encrypted data. Anonymous HIBE get linear size private keys and constant size ciphertext. Weakness is without using hidden structures, it is not as fast as possible to search keywords.

Gentry C. [8] presents an Identity Based Encryption (IBE) system that is fully secure in the standard model. He presented a fully secure IBE system that is quite practical, has very compact public parameters, and has a tight security reduction. It is recipient-anonymous, and its proof extends Cramer- Shoup-type techniques to IBE systems. It remains an outstanding open problem to construct a fully secure IBE system without random oracles that has a tight reduction based on a more natural assumption. Another interesting problem is to construct a hierarchical IBE system that has a reduction based on a reasonable assumption, either in the standard model or the random oracle model, that is polynomial in q and the number of levels.

3. 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. One of the prominent works to accelerate the search over encrypted keywords in the public-key setting enabling search over encrypted keywords to be as efficient as the search for unencrypted keywords, such that a cipher text containing a given keyword can be retrieved in time complexity logarithmic in the total number of all cipher texts.

This is reasonable because the encrypted keywords can form a tree-like structure when stored according to their binary values. However, 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. 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. Observe that a keyword space is usually of no high min-entropy in many scenarios. Semantic security is crucial to guarantee keyword privacy in such applications. Thus the linear search complexity of existing schemes is the major obstacle to their adoption. Unfortunately, the linear complexity seems to be inevitable because the server has to scan and test each cipher text, due to the fact that these cipher texts are indistinguishable to the server.

3.1 Disadvantages Of Existing System

Each sender should be able to generate the keyword-searchable cipher texts with the hidden star-like structure by the receiver's public-key, the server having a keyword search trapdoor should be able to disclose partial relations, which is related to all matching cipher texts. Semantic security is preserved, if no keyword search trapdoor is known, all cipher texts are indistinguishable, and no information is leaked about the structure, and given a keyword search trapdoor, only the corresponding relations can be disclosed, and the matching cipher texts leak no information about the rest of cipher texts, except the fact that the rest do not contain the queried keyword.
The integrity of data is not possible in existing system
An existing system public verifier does not check the data in multi cloud

4. PROPOSED SYSTEM

In proposed scheme, 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. Construct a simple SPCHS from scratch in the random oracle model. The scheme generates keyword-searchable ciphertexts with a hidden star-like structure. The search performance mainly depends on the actual number of the ciphertexts containing the queried keyword.

A generic SPCHS construction is to generate keyword-searchable cipher texts with a hidden star-like structure. Generic SPCHS is inspired by several interesting observations on Identity-Based Key Encapsulation Mechanism (IBKEM). Build a generic SPCHS construction with Identity Based Encryption (IBE) and collision-free full-identity malleable IBKEM. The resulting SPCHS can generate keyword-searchable cipher texts with a hidden star-like structure. Moreover, if both the underlying IBKEM and IBE have semantic security and anonymity, the resulting SPCHS is semantically secure. As there are known IBE schemes in both the RO model and the standard model, an SPCHS construction is reduced to collision-free full-identity malleable IBKEM.

4.1 Advantages Of Proposed System

IBKEM schemes to construct Verifiable Random Functions. One of these IBKEM schemes is anonymous and collision-free full identity malleable in the RO model utilized the approximation of multilinear maps to construct a standard-model version of Boneh-and-Franklin IBE scheme.
Transform this IBE scheme into a collision-free full-identity malleable IBKEM scheme with semantic security and anonymity in the standard model. Hence, this new IBKEM scheme allows us to build SPCHS schemes secure in the standard model with the same search performance as the previous SPCHS construction from scratch in the RO model. Each client has a private correspond to his identity such as name, id or any. The public verifier allow the user to correspond to his identity such as private Key.

5. IMPLEMENTATION

5.1 Modeling SPCHS

Hidden structure formed by ciphertexts as (C,Pri,Pub), where C denotes the set of all ciphertexts, Pri denotes the hidden relations among C, and Pub denotes the public parts. In case there is more than one hidden structure formed by ciphertexts, the description of multiple hidden structures formed by ciphertexts can be (C, (Pri_1,Pub_1),..., (Pri_N,Pub_N)), where N € **N.** Moreover, given (C,Pub_1,...,Pub_N) and (Pri_1,...,Pri_N) except (Pri_i, Pri_j) (where i ≠ j), one can neither learn anything about (Pri_i, Pri_j) nor decide whether a ciphertext is associated with Pub_i or Pub_j .

In SPCHS, the encryption algorithm has two functionalities. One is to encrypt a keyword, and the other is to generate a hidden relation, which can associate the generated ciphertext to the hidden structure. Let (Pri,Pub) be the hidden structure. The encryption algorithm must take Pri as input, otherwise the hidden relation cannot be generated since Pub does not contain anything about the hidden relations. In addition, SPCHS needs an algorithm to initialize (Pri,Pub) by taking the master public key as input, and this algorithm will be run before the first time to generate a ciphertext. With a keyword search trapdoor, the search algorithm of SPCHS can disclose partial relations to guide the discovery of the ciphertexts containing the queried keyword with the hidden structure.

SPCHS consists of five algorithms:

1.SystemSetup(1^k,W): Take as input a security parameter 1^k and a keyword space W, and probabilistically output a pair of master public-and-secret keys (PK,SK), where PK includes the keyword space Wand the ciphertext space C.

2.StructureInitialization(PK): Take as input PK, and probabilistically initialize a hidden structure by outputting its private and public parts (Pri,Pub).

3.StructuredEncryption(PK,W,Pri): Take as inputs PK, a keyword W € W and a hidden structure's private part Pri, and probabilistically output a keyword searchable ciphertext C of keyword W with the hidden structure, and update Pri.

4.Trapdoor(SK,W): Take as inputs SK and a keyword W € W, and output a keyword search trapdoor T_W of W.

5.StructuredSearch(PK,Pub,C,T_W): Take as inputs PK, a hidden structure's public part Pub, all keyword-searchable ciphertexts **C** and a keyword search trapdoor T_W of keyword W, disclose partial relations to guide finding out the ciphertexts containing keyword W with the hidden structure.

An SPCHS scheme must be consistent in the sense that given any keyword search trapdoor T_W and any hidden structure's public part Pub, algorithm StructuredSearch(PK,Pub,**C**,T_W) finds out all ciphertexts of keyword W with the hidden structure Pub.

Search algorithm has two functionalities.

1. Algorithm Trapdoor allows the receiver to delegate a keyword search trapdoor to the server.
2. StructuredEncryption

Advantage of an algorithm is that anyone who knows the receiver's public key can upload keyword-searchable ciphertexts to a server.

5.2 SPCHS Architecture

In SPCHS, Data Owners communicate and post data in Cloud Server. With the knowledge of cloud server, users can directly contact with Authority Audit / Authentication Audit (AA) using secret key. Public Key (PK) having only Authenticate id (aid) and Secret key (SK) having user id (uid) & Authenticate id(aid). Keyword can be search using public key cipher text model. Whenever gives an authentication, secret key will receive through mail, then only right person can access data. Figure 6.1 illustrating the architecture diagram.

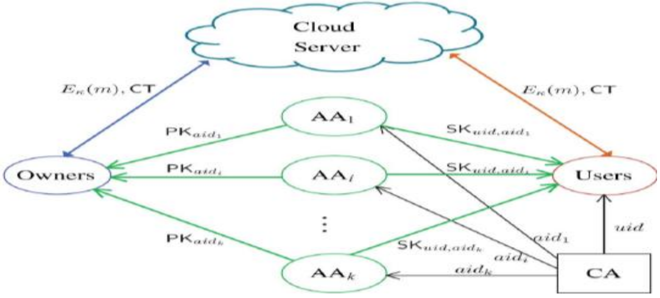

Fig.1 Architecture Diagram

5.3 IBKEM Algorithm

Formalize collision-free full-identity malleable IBKEM and a generic SPCHS construction from IBKEM. Our generic construction also relies on a notion of collision-free full-identity malleable IBKEM. Take the random value as an input of the algorithm.

IBKEM Consists of Four Algorithms:

1. $\text{Setup}_{\text{IBKEM}}$ (1^k, ID_{IBKEM})

Take as inputs a security parameter 1^k and an identity space ID_{IBKEM} , and probabilistically output the master public-and-secret-keys pair(PK_{IBKEM} , SK_{IBKEM}) , where PK_{IBKEM} includes the identity space ID_{IBKEM}, the encapsulated key space K_{IBKEM} and the encapsulation space C_{IBKEM}.

2. $\text{Extract}_{\text{IBKEM}}$ (SK_{IBKEM}, ID)

Take as inputs SK_{IBKEM} and an identity ID € ID_{IBKEM}, and output a decryption key $\hat{S}_{\text{ID}}$ of ID.

3. $\text{Encaps}_{\text{IBKEM}}$ (PK_{IBKEM}, ID, r)

Take as inputs PK_{IBKEM}, an identity ID € ID_{IBKEM} and a random value r, and deterministically output a key-and-encapsulation pair ($\hat{Y}$, $\hat{C}$) of ID.

4. $\text{Decaps}_{\text{IBKEM}}$ ($\hat{S}_{\text{ID}}{}^1$, $\hat{C}$)

Take as inputs the decryption key $\hat{S}_{\text{ID}}{}^1$ of identity ID^1 and an encapsulation $\hat{C}$, and output an encapsulated key or _ , if the encapsulation is invalid.

An IBKEM scheme must be consistent in the sense that for any
($\hat{Y}$, $\hat{C}$) = $\text{Encaps}_{\text{IBKEM}}$ (PK_{IBKEM}, ID, r) , $\text{Decaps}_{\text{IBKEM}}$ ($\hat{S}_{\text{ID}}{}^1$, $\hat{C}$) = $\hat{Y}$ holds if ID^1 = ID, except with a negligible probability in the security parameter k.
The collision-free full-identity malleable IBKEM implies the following characteristics. They are all identities decryption keys can encapsulate the same encapsulation, all encapsulated keys are collision-free, the generator of the encapsulation can also compute these encapsulated keys, the encapsulated keys of different encapsulations are also collision-free.
IBKEM is collision-free full-identity malleable, if there is an efficient function FIM that for any ($\hat{Y}$, $\hat{C}$) = $\text{Encaps}_{\text{IBKEM}}$ (PK_{IBKEM}, ID, r).
The function FIM satisfies the following features
Full-Identity Malleability - For any identity ID^1 € ID_{IBKEM} ,the equation FIM(ID^1, r) = $\text{Decaps}_{\text{IBKEM}}$ ($\hat{S}_{\text{ID}}{}^1$, $\hat{C}$) always holds, where $\hat{S}_{\text{ID}}{}^1$ = $\text{Extract}_{\text{IBKEM}}$ (SK_{IBKEM}, ID^1)
Collision Freeness - For any identity ID^1 € ID_{IBKEM} and any random value r^1, if ID ≠ ID^1 ∨ r ≠ r^1, then FIM (ID, r) ≠ FIM(ID^1, r^1) holds, except with a negligible probability in the security parameter k.
A collision-free full-identity malleable IBKEM scheme may preserve semantic security and anonymity. Incorporate the semantic security and anonymity into AnonSS-ID-CPA secure IBKEM. But this security is different from the traditional version of the Anon-SS-ID-CPA security due to the full-identity malleability of IBKEM.

5.4 Modules Description

This project consists of four modules. They are User Module, Identity Based Encryption, Fast Searchable Encryption and Semantic Data Security.

6.4.1 User Module

ADMIN
In Admin module is used to help the server to view details and upload files with the security. Admin upload the data's to database. Also view the subscriber details and user details. Admin find the redistribute details. Also who send the data and receive the data's. Data owner store large amount of data to clouds and access data using secure key provided admin after encrypting data's. Encrypt the data using Secret Key. User store data after auditor, view and verifying data and also changed data. User again views data at that time admin provided the message to user only changes data.

PROVIDER
In Provider module subscriber choose document and download the data's from service providers. Subscribers pay the amount to service provider. Service provider provides that data key to subscriber. So subscribers download the data using data key. A cloud computing service provider serves users' service requests by using a server system, which is constructed and maintained by an infrastructure vendor and rented by the service provider.

USER
In User module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first user can register their details like user name, password, email, mobile no, and then. We develop this module, where the cloud storage can be made secure.

5.4.2 Identity Based Encryption

Batch identity-based key distribution is a direct application of collision-free full-identity malleable IBKEM is to achieve batch identity-based key distribution. In such an application, a sender would like to distribute different secret session keys to multiple receivers so that each receiver can only know the session key. With collision-free full-identity malleable IBKEM, a sender just needs to broadcast an IBKEM encapsulation in the identity based cryptography setting, that is encapsulating a session key K to a single user ID. According to the collision freeness of IBKEM, each receiver ID0 can decapsulate and obtain a different key K0 with secret key in the identity based crypto-system. Due to the full-identity malleability, the sender knows the decapsulated keys of all the receivers.
Anonymous identity-based broadcast encryption is a slightly more complicated application is anonymous identity-based

broadcast encryption with efficient decryption. An analogous application was proposed respectively application will work if the IBKEM is collision-free full-identity malleable.

5.4.3 Fast Searchable Encryption

As-fast-as-possible search in PEKS with semantic security. the concept of SPCHS as a variant of PEKS. The new concept allows keyword-searchable ciphertexts 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 ciphertexts of the queried keyword.

The scheme generates keyword-searchable ciphertexts with a hidden star-like structure. It has search complexity mainly linear with the exact number of the ciphertexts containing the queried keyword. It outperforms existing PEKS schemes with semantic security, whose search complexity is linear with the number of all ciphertexts.

Two collision-free full-identity malleable IBKEM instances, which are respectively secure in the RO and standard models. SPCHS seems a promising tool to solve some challenging problems in public-key searchable encryption. One application may be to achieve retrieval completeness verification has not been achieved in existing PEKS schemes.

5.4.4 Semantic Data Security

The SS-CKSA security of the SPCHS scheme relies on the DBDH assumption in Even in the case that a sender gets local privacy Pri compromised, SPCHS still offers forward security. This means that the existing hidden structure of ciphertexts stays confidential, since the local privacy only contains the relationship of the new generated ciphertexts. To offer backward security with SPCHS, the sender can initialize a new structure by algorithm Structure Initialization for the new generated ciphertexts. A collision-free full-identity malleable IBKEM scheme may preserve semantic security and anonymity.

6. CONCLUSIONS

This project investigated as-fast-as-possible search in PEKS with semantic security. The concept of SPCHS as a variant of PEKS. New concept allows keyword-searchable ciphertexts 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 ciphertexts 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. The scheme generates keyword-searchable ciphertexts with a hidden star-like structure. It has search complexity mainly linear with the exact number of the ciphertexts containing the queried keyword. It outperforms existing PEKS schemes with semantic security, whose search complexity is linear with the number of all ciphertexts. Collision-freeness and full-identity malleability in some IBKEM instances, and formalized these properties to build a generic SPCHS construction. Two collision-free full-identity malleable IBKEM instances, which are respectively secure in the RO and standard models. SPCHS seems a promising tool to solve some challenging problems in public-key searchable encryption.

ACKNOWLEDGEMENT

I would like to thank my project guide Ms. S. Nithya dhevi, Assistant Professor, CSE Dept., she served as sounding board for both contents and programming work. Her valuable and skillful guidance, assessment and suggestions from time to time improved the quality of work in all respects.

REFERENCES

1. Arriaga A.et al. (2014): Trapdoor Privacy In Asymmetric Searchable Encryption, In: AFRICACRYPT 2014. LNCS, vol. 8469, pp. 31-50.

2. Ateniese G., Gasti P. (2009): Universally Anonymous IBE Based on the Quadratic Residuosity Assumption. In: Fischlin M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 32-47.

3. Bellare M.et al. (2007): Deterministic and Efficiently Searchable Encryption. In: Menezes A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 535-552.

4. Boneh D.et al. (2004): Public Key Encryption with Keyword Search. In: Cachin C., Camenisch J.(eds.) EUROCRYPT 2004.LNCS, vol.3027, pp.506-522.

5. Boneh D.et al. (2004): Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223-238.

6. Boyen X.et al (2006): Anonymous Hierarchical Identity-Based Encryption. In: Dwork C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290-307.

7. Ducas L.(2010): Anonymity from Asymmetry:New Constructions for Anonymous HIBE. In:Pieprzyk.J.(ed.). LNCS, vol.5985, pp.148-164.

8. Gentry C. (2006): Practical Identity-Based Encyrption Without Random Oracles. In:Vaudenay S.(ed.) EUROCRYPT 2006., vol.4004, pp.445-464.