Journal of Theoretical and Applied Information Technology
15th November 2017. Vol.95. No 21
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EXPERIMENTAL RESULTS ON MULTI-KEY SEARCHABLE ENCRYPTION TECHNIQUE WITH DIFFERENT ELLIPTIC CURVES AND APP DESIGNING

[1*]PUTTA SRIVANI, [2]SIRANDAS RAMACHANDRAM, [3]RANGU SRIDEVI

[1]Research Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India.
[2] Professor, Department of Computer Science and Engineering, Osmania University, Hyderabad, Telangana, India.
[3]Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India.
Email: [1*]pulla.srivani@gmail.com, [2]schandram@gmail.com, [3]sridevirangu@gmail.com

ABSTRACT

Multi-Key searchable encryption scheme is a technique implemented to perform the keyword search on cipher text. This scheme can be practically applied for client server applications to achieve data confidentiality and allows the server to perform the operation like search on the cipher data. Experimental results of multi-key searchable encryption scheme implemented for different types of elliptic curves are shown in this paper and results are compared between different types of elliptic curves. An application also designed with Java as frontend and MongoDB as backend. It also shows the search time taken to perform the search operation on the encrypted data by using this scheme.

Keywords: *Encryption, Search Token, Delta, Token, Cloud, Multi-key*

I. INTRODUCTION

Cloud computing is a network delivers some computing services like software, servers, databases, storage etc based on pay as per you use. When we use the cloud for data storage, the problem identified is –In what way the information is stored in the cloud and how the information is retrieved from the cloud. When cloud is allowed to store plain text data, there is a chance of leaking of information. Hence Data Storage and Information Retrieval is a big challenging issue. One promising approach to achieve confidentiality is outsourcing only encrypted data. In single user applications the client stores the encrypted data at the server and performing encryption and decryption only on the client side. In multi-user applications, each user can access the documents, which he has access to, saved on the server. Each user file is encrypted with a different key and made accessible of the file keys to the corresponding users. One challenging issue is to allow the user to perform the search operation on the encrypted files. Many web applications like chat, document sharing, forums, calendars and assignment submission apps support to perform the operation like search on the encrypted files shared by different users. Earlier, the researchers work done on searchable encryption techniques would require the server to provide search token by the client under each key of all the documents he has access to. But such schemes performance may be slow down when huge number of documents has to be searched by the server.

Multi-Key Searchable Encryption Scheme[12] allows the server to use a single token provided by the client to perform the search operation on all the documents he has access to encrypted with different keys.

In this scheme, encryption and decryption is performed at the client side. This scheme allows the server to perform the search operation on encrypted data. In this scheme, the client provides only a single token , generated to that search word, to the server. The server uses this token and converts into a search token for all the documents encrypted with different keys. The main advantage

in this scheme is transferring only a single token of that search word to the server.
It avoids the transmission of different search tokens used for different documents It also provides security to the data as the search operation is performed on encrypted data.

The two challenging issues in this scheme is that there is no trusted third party for the distribution of the keys and it can be implemented for real time web applications. We present the experimental results of this scheme under different elliptic curve parameters. An application has designed with MongoDB as back end and java as frontend by implementing this scheme. We estimated the time taken to perform the search operation on encrypted data for lakh records. This scheme has implemented with different elliptic curve and estimated the time taken under each elliptic curve

2. GENERAL MODEL OF SEARCHABLE ENCRYPTION METHOD

As we know that the cloud is widely used for backups, the data has to be stored in unreadable form to reduce the risks like privacy. Earlier, to perform the search operation by the user, the query is sent to the server. The documents are decrypted at the server side and the search operation is performed on the plain text. In this approach, the time consumption is more. To reduce time consumption, the search operation is performed on the cipher text by the server. This search is known as Searchable encryption.

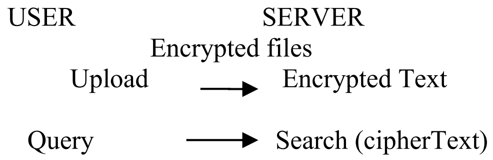

Fig.1. Searchable Encryption Method-A General Model

3. LITERATURE SURVEY ON SEARCHABLE ENCRYPTION SCHEMES

Encryption is the technique to maintain privacy to the data. Performing the search operation on cipher text is a challenging issue. A number of searching techniques had been implemented to perform the search operation on the cipher text when the data is outsourced. i.e cloud computing.

Multi - key word ranked search has traditionally been provided by Information Retrieval system (IRS) for data user. To overcome the problem of searching on cipher text, an algorithm has been proposed by[1], which performs the search operation for multi keyword over encrypted data using Semantic-Analysis, which returns the file containing the keyword search based on the Semantic Analysis.

All the Searchable encrypted schemes over encrypted databases are limited to single user settings. To support multiuser searches, Feng Bao, Robert H. Deng, Xuhua Ding, Yanjiang Yang[2] has generated a system model with a set of security requirements to provably satisfy those requirements. In their designed model, a distinct key is assigned to each user, and consequently, any users authorized cancellation does not require to re-encrypt the database and updating of query keys, and is transparent to the user who are non revoked. Moreover, users who are authorized can perform insertion operation and search the database, which is an important feature in the multi-user setting to share the data.

Dan Boneh, Giovanni,Rafail Ostrovsky and Guiseppe[3] proposed a concept to perform the search operation on cipher data by using a system called public key system. Let us consider the user Alice want to send email to user Bob encrypted by using Bob's public key. For example, an email server wants to test whether the mail has a keyword called 'resign'. As the emails are in the encrypted form, the email server is not having the ability to perform the search on cipher data. So, they designed a scheme that enables Bob to provide a key to the email server. The server generates a trapdoor for the word by using the key and performs the test. The server simply publishes the results to the Bob whether the word 'urgent is present or not.

Reza Curtmola, Juan Garay, Seny Kamara, Rafail Ostrovsky [4] has proposed two new searchable symmetric encryptions and these can be applied for multiuser settings under secure constructs.

Eu-Jin Goh [5]has developed an efficient secure index schene called Z-INDEX constructed using Bloom filters and pseudo-random functions, and explains how to implement Z-INDEX to perform searches on encrypted data. These techniques can be implemented for building searchable encrypted audit logs, private query database schemes, set membership tests.which are secured and hashing schemes.

Seny Kamara, Charalampos Papamanthou, Tom Roeder [6] has proposed Dynamic Searchable Symmetric Encryption scheme which allows to perform deletions and additions of files from the database. Using tokens, all these operations are handled in this scheme. The client generates an add token which the server uses to update the encrypted index for addition of a file. The client generates a delete token which the server uses to delete the encrypted index for deletion of a file.

Dawn Xiaodong Song David Wagner Adrian Perrig[7] has proposed four cryptographic searchable schemes that enables to perform search on cipher data without leaking plain text to the server. These schemes support sequential scan, Controlled Searching, Hidden Searches.

Subsequently, Goh [5] and Chang and Mitzenmacher [8] has designed the scheme to perform the search operation on cipher text indexes generated for a group of documents. With constructed indexes, their schemes improved the search efficiency for a large storage. Efficiency measured between the bit-length generated for each document index and the total number of keywords is proportional. Dan Boneh, Xavier Boyen, Eu-JinGoh[13] has developed a scheme called Hierarchical Identity Based Encryption system to perform the constant size cipher text search operation. This scheme supports the number of applications like converting the NNL broadcast encryption scheme into public key Broadcast CryptoSystem, an efficient mechanism for encrypting to the future, forward public key secure cryptosystem.

Seny Kamara charalampos papamanthou[14] has designed a SSE scheme called Parallel and Dynamic searchable Symmetric Encryption to perform parallel search and it takes O(r) parallel time , where r denotes the document count, to search a keyword 'w'. This scheme also achieved the properties like security against adaptive chosen keyword attacks, external memory implementation etc. This scheme uses non-linear data structure called red-black trees and its construction is based on random oracle model.

Ostrovsky and skeith[15] has done the work on private stream searching that allows the client to perform the search query that is encrypted. The server searches in a stream of plain data by using this query. The matching documents are returned by the server to the client by unknowing about the query.

Curtmola et.al [16] has proposed two schemes where an inverted index is generated for each distinct word instead of creating for each file. This idea reduces the search time to refer all the indexes generated for each file. This scheme is optimal and sub linear and achieves IND-CKA security also. Golle et. al.[17] poineered a scheme called "conjunctive Keyword Search" that supports to search a group of keywords in a single query. An assumption that there exists keyword fields for each document. The user performs the search by using these keyfields. This scheme achieves IND1-CKA security in the Random Oracle Model.

Park et. al. [18] pioneered a method to perform the search for keywords over encrypted data with errors. This scheme idea is to compute encryption character by character of each word and then apply Hamming Distance for searching similar keywords. As the encryption has done character-wise, it is not secure. Hence security has been improved in new versions of this scheme. PKL$^+$-(I,II) algorithms are more efficient and secure . These algorithms uses Pseudo-Random Functions(PRF), generators, exponentiations and one way functions. PKL$^+$-I needs one hash for each character of a word. PKL$^+$-II needs hash and PRF for each character of a word. These two versions calculates the Hamming Distance between the keyword and the pattern to do search operation.

Yang et.al.[19] pioneered a scheme that uses bilinear mapping for keyword search in multi user settings. Using bilinear symmetric mapping of prime order, the scheme has been designed. Yang et.al. idea is that the server can compute a common key by using user's trapdoor and user' helper key to search the index. This scheme requires to compute bilinear mapping and pairing for each keyword search. This scheme is proven secure under the two assumptions-DDH and CDH in the Random Oracle Model.

The idea of Crescenzo and Saraswat is to design MultiWriter scheme to perform the search operation on encrypted data. They pioneered a scheme called "Public Key Encryption with Keyword search by using Jacobi symbols. This scheme is not based on bilinear mapping and it implements cock's Identity Based Encryption . Its efficiency has been proved by considering 4m Jacobi symbols per keyword to encrypt the data where m=160 bits that denotes the size of the keyword in bits.

The research work done on searchable encryption schemes mainly focuses on how search operation can be done when the information is encrypted with the same key. Some schemes are public key cryptosystems and others secret key cryptosystems. Only the researcher Lopez-Alt et al.[21] has designed a searchable encryption scheme with different keys. Their scheme called "Fully homomorphic encryption " scheme supports any type operation to be performed on encrypted data. All the users can compute a function on encrypted data with their keys. The drawbacks are time consuming , running MPC protocol by coming all parties together and a client needs to do some work related to retrieving all the keys. Multi key searchable encryption scheme avoids these drawbacks.

Another research work done by Bao et al.[2] Is related to performing the search operation on encrypted data where all the documents are encrypted with one key. In his scheme , though each user has a different key, the documents are encrypted with one key. The drawback of this scheme is it cannot be applied directly to multi-key setting. Some of the schemes described in [22,23,24] have similar properties and fall i the group of multi-user one-key scheme.

Advantages of Multi key searchable encryption algorithm is that can be applied to multi-key settings in multi user environment. We can avoid the distribution of different keys to the server where these are used to encrypt different documents.

4. ELEMENTARY CONCEPTS ON ELLIPTIC CURVES

4.1 Introduction

Let the field of integers modulo q is denoted by Fq where ‘q’ is a prime number. An elliptic curve EC over[9] a finite field Fq is denoted by an equation

$$i^2 = j^3+aj +b$$

where a, b belongs to Fq satisfy the condition

$$4a^3 +27b^2 \equiv 0 \ (\mathrm{mod}\ q).$$

A pair (j, i), is a point on the curve where $j,i \in Fq$ and the point (j, i) should satisfy the equation. Let ‘∞’ represents ‘point at infinity’, is also said to be on the curve. A group of all the points on EC is denoted by EC(Fq). An elliptic curve EC over F7 with an equation $i^2= j^3 +2j +4$, then EC(F7) = {∞, (0,2), (0,5), (1,0), (2,3), (2,4), (3,3), (3,4), (6,1), (6,6)} are the points on EC.

4.2 Elliptic Curve Key Generation

Let Fq defines a finite field of an elliptic curve EC. Let ‘P’ be a point in EC(Fq), and let ‘P’ has prime order n. Let EC(Fq) represents cyclic subgroup formed by ‘P’ is

$$P= \{\infty, P,2P,3P,...,(n-1)P\}.$$

Let q, EC, P are the public domain parameters denotes the prime number, elliptic curve equation and the point with order ‘n’ respectively. Let ‘m’ is an integer private key selected from the range of values [1, n-1] uniformly at random. Let Q=mP is the corresponding public key.

4.3 Bilinear Mapping On Elliptic Curve Group

A mapping is defined between a pair of points on an additive elliptic curve EC over some field ‘n’ and an element of the multiplicative group with finite extension ‘N’. It is called bilinear mapping (e)[10] represented as an equation $e(aC, bD) = e(C, D)^{ab}$ where C,D denote elliptic curve points and a, b are the integers.

Modified Weil pairing and Tate pairing are the algorithms used for cryptographic bilinear mapping.

4.4 Types Of Elliptic Curves

Type A curve: An elliptic curve with equation $y^2=x^3+x$ is called Type A curve.
Let Field ‘F_pq‘ is used to construct the pairings where ‘pq’ is some prime number pq= 3 % 4. Let G1, G2 are called the group of points(E(F_pq)) on elliptic curve where pairings are constructed between them. So, symmetric pairing is formed between them. It shows # E(F_pq)=pq+1 and #E(F_pq^2)=(pq+1)^2. So ‘2’ is the the embedding degree and GT forms a subgroup of F_pq^2 and ‘r’ is called the order of some prime factor ‘pq+1’.

Type B curve: An elliptic curve with equation $y^2=x^3+1$ is called Type B curve. Let the field F_pq is used to construct the pairings where ‘pq’ is some prime number pq=2 mod 3. To compute cube roots, it is easy in F_pq. By constraining ‘pq’ appropriately, we can achieve it for Type A pairing also.

Type C curve: Type ‘C’ curves are called super singular curves with curve equations $y^2=x^3+2x-1$ and $y^2=x^3+2x+1$. These curves are constructed over a ‘3’ characteristic field. These curves are implemented for generating short signatures from weil pairing. We can speed up the pairings by applying the optimization techniques.

Type D curve: Type D curves are known as ordinary curves with curve equation $y^2=x^3+ax+b$. Type D curves are constructed with some field and order h*r. ‘h’ is a small value and ‘r’ is called prime number

Type E curve: Type E curves satisfies the Diophantine equation $DV^2=4q-t^2$ constructed by

Complex Multiplication Method. If q=D r^2h^2+1and 't' has a value 2 for some integer 'h' and prime number 'r'. This equation can be solved with V=2rh. Type D curve has order q-1. Note power (r ,2) divides q-1, and these curves has '1' as embedding degree. The size of the 'q' is 1024 bits and a lot of memory is required for group elements to represent. Type D curves leads to slow pairing if optimizations are applied to this curve

Type F curve: These curves takes the form E: $y^2= x^3+ b$. Pairings can be formed with an embedding degree '12'. An embedding degree can be represented with 'k' and these curves need only 160 bits to denote the elements of one group. If curves are constructed with an embedding degree of '12', it allows short signatures with higher security.

Type G curve: Elliptic curves constructed with equation $y^2=x^3+ax+b$ are called Type G curves constructed by complex multiplication method. These curves are defined with an order 'h*r'.

Type I curve: Type I curves are called super singular curves take the form $Y^2=X^3-X+1$ with a finite Field of F_(3^n). An Embedding Degree '6' is implemented for these curves. Let G1, G2 form the group of points (F_3^n) and a subgroup of F_(3^n) is denoted with GT.

5. SCHEME

Let us elaborate the implementation of Multi-Key Searchable Encryption Scheme for 'n' users. Let each user 'i' has a public key denoted as puk^i. Let K_j denote the key of the document 'j' created by the user 'i'. For example, say Bob has 'n' documents encrypted and stored at the server side by using a key k_j for each document where j=1 to n. He want to perform the search operation on all the documents he has permission to find a word 'w'. So, he generates a token for a search word by using his public key and transmits it to the server. To perform the search operation by the server, he provides the public data called DELTA VALUES generated for each key 'k_j' and represented as $\Delta puk_i K_j$. The server receives the token for a search word and the DELTA VALUES from him. The server adjusts the search token generated using his public key to a search token under k_j by using DELTA VALUES. By this procedure, the server can generate the search tokens for all the documents by using DELTA VALUES to perform the search operation on all documents. As only single key is provided to the server, this scheme is an efficient scheme for search operation.

In this paper, scheme is implemented with all types of elliptic curves and a comparison has brought between them with respect to time.

6. CONSTRUCTION

Let H1: {0,1} → G1 and H2: GT X GT → {0,1} denote the hash functions used in this scheme and modeled as random oracles. Multi-Key Searchable Encryption follows as:

- params ← MKY.Setup(1^k): return (p, G1, G2, GT, e, g1, g2, gT) ← CSetup(1^k).

MKY.Setup(1^k): It is a function used to set the curve parameters.

- puk ← MKY.KeyGen(params):
  return puk ← Zp.

It is a function used to generate the public key.

- K1 ← MKY.KeyGen(params): return k1 ← Zp.

MKY.KeyGen(params): It is a method used to generate the 'K1' key. To encrypt the text file, this key is used.

- Δ ← MKY.Delta(puk, k1): return $\Delta = g^{k1/puk} \in G2$.

MKY.Delta(puk, k1): It is a function used to generate the delta value. Delta is generated by using public key puk and the 'k1' key. User computes the 'delta' and passes to the server.

- tk ← MKY.Token(puk,w): return $tk = H(w)^{puk} \in G1$.

MKY.Token(puk,w): It is a function used to generate the token between the keyword 'w' and the public key 'puk'.

- c ← MKY.Enc(puk,w): Draw r ← GT . Output c = (r,H2(r, e(H(w), g2)^{puk}))

MKY.Enc(puk,w): It is a function used by the client to perform the encryption for a word.

- tk′ ← MKY.Adjust(tk, Δ): return tk′ = e (tk, Δ) ∈ GT.

MKY.Adjust(tk, Δ): It is a function used to generate the search token 'tk'.

- bit ← MKY.Match(tk, ct): Let ct = (r, n). Return H2(r, tk)? =n.

MKY.Match(tk, ct): It is a function used to compare the search word with the encrypted text file. It returns true if the keyword in the file is found else false.

.

7. EXPERIMENTAL RESULTS

Multi-Key Searchable Encryption Scheme is implemented for different elliptic curves and a comparison has been brought between the different elliptic curves implementations.

Algorithm has implemented in 'C' and used the PBC library[11] with different (pairing parameters) elliptic curves under ubuntu operating system. Below are the experimental results on an Intel i3 processor -3120M CPU @ 2.50 GHZ running on dual core.

When the algorithm is implemented with different elliptic curves, Type D curve implementation took less time when compared to all types of curve implementation .

Table 1 Multikey Searchable Encryption Algorithm Implemented With All Types Of Elliptic Curves With Time

Algorithm	Type A	Type A1	Type D with 159 no. of bits in q	Type D with 201 no. of bits in q	Type D with 224 no. of bits in q	Type D with 105171-196-185	Type D with 277699-175-167	Type D with 278027-190-181	Type E	Type F	Type G
Time(s)	0.041679	0.178408	0.29105	0.048337	0.050077	0.041106	0.037007	0.037233	0.053924	0.096890	0.090783

8. IMPLEMENTATION

This scheme can be implemented for designing the applications in the cloud environment like chat applications, home work assignment, big data analytics apps like marketing and advertising, data storage apps that supports storing and retrieving of required data etc to perform the sequential search operation on the cipher text. An app is designed with front end language as java and MongoDB as backend. One lakh records are generated randomly by using JSON online generator. This app is designed to estimate the time taken to perform sequential search operation on encrypted documents. This application has implemented with three collections.

a) collection named Restaurant

b) collection named Rest

c) collection named delta

a) Restaurant collection is used to store the plain text documents that are generated randomly by using JSON online generator. This collection has four columns.

*Object_ id
* name
* address
*restaurant_id

Object_id: This column is used to store the id for each document. It is generated implicitly in MongoDB.

Name: This column is used to the names of the restaurants.

Address: It is used to store the address of the restaurant.

Restaurant_id: It is used to store the id of the restaurant.

b) Rest collection is created to store the encrypted documents. It has three columns

*id
*name_key
*name

Id : It is a column used to store the object id of the document. It is automatically generated by MongoDB.

Name_key: It is a column used to store the encrypted names of the restaurants that are present in the Restaurant collection under the column 'name'. This column is used to perform the search operation.

Name: It is a column used to store the names of the restaurants for verification purpose.

c)delta collection is used to store the delta values. These values are used in the search operation. It has three columns.

*id
*delta
* key

Id: It is a column used to store the object id of the document. Its values are generated implicitly by MongoDB.
Delta: It is a column used to store the delta values. Deltas are generated by using two keys.i.e. public key of the user and key of the document used for encryption.
Key: It is a column used to store the keys of the documents used for encryption. Each document of the 'name' column of the Restaurant collection is encrypted with these keys values respectively.
. Table 2 shows the experimental results of the app designed to perform the sequential search operation on the Cipher text by using this scheme.

Table 2 Experimental Results On Intel Processor On Dual Core System

No. Of documents	1000	2000	10000	20000	30000	50000	100000
Time to perform the search(in milliseconds)	250	150	600	820	383382	3560000	7100000

9. CONCLUSION

Limitation of this algorithm is that it can be implemented for sequential search operation on encrypted data. Further, it can be enhanced to index based search operation on encrypted data. The above system has designed to perform the search on encrypted data. We conducted an experiment on Multi-key Searchable Encryption Scheme with different elliptic curve parameters by using pbc library. The experimental results show that Type D curve parameters took less time i.e. 0.037007 s when compared with other curves. An application also designed with java as front end and MongoDB as backend for one lakh records and implemented this scheme for Type 'D' curve to estimate the time to perform the search operation on cipher text .

10. DISCUSSIONS AND FUTURE WORK

The main objective is- how to perform the search operation on encrypted data. Some research work done by authors have designed the algorithms that supports the search operation when the information is encrypted with the same key. These schemes cannot be applied to a multi-key setting in real time applications. Some other schemes fall in the group of multi-user one-key schemes. Multi-key searchable encryption scheme can be implemented to multi-user setting where the documents are encrypted with different keys. Still this scheme can be enhanced to implement for index based searching.

REFERENCES

[1] Li Chen, Xingming Sun, Zhihua Xia,Qi Liu,"An Efficient and Privacy-Preserving Semantic Multi-Keyword Ranked Search over Encrypted Cloud Data" in International Journal of Security and Its Application in 2014

[2] Feng Bao, Robert H. Deng, Xuhua Ding, and Yanjiang Yang. Private query on encrypted data in multi-user settings. In ISPEC, pages 71–85, 2008.

[3] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, ''Public Key Encryption with Keyword Search,'' in Proc. EUROCRYPT, 2004, pp. 506-522.

[4] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, ''Searchable Symmetric Encryption: Improved Definitions and

Efficient Constructions,'' in Proc. ACM CCS, 2006, pp. 79-88.

[5] E.-J. Goh, ''Secure Indexes,'' in Cryptology ePrint Archive,2003[Online].Available: http://eprint.iacr.org/2003/216

[6] Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic searchable symmetric encryption. In CCS, pages 965–976, 2012.

[7] Dawn Xiaodong Song, DavidWagner, and Adrian Perrig. Practical techniques for searches on encrypted data., In Proceedings of the 21st IEEE Symposium on Security and Privacy, Oakland, CA, May 2000.

[8] Y. Chang and M. Mitzenmacher, Privacy Preserving Keyword Searches on Remote Encrypted Data. Proc. Applied Cryptography and Network Security, ACNS'05, LNCS 3531, pp. 442-455, 2005.

[9] D.R.Hankerson,A.J.Menezes and S.A Vanstone, Guide to elliptic curve cryptography. springer-verlog, New York 2004.

[10]https://hal.archives-ouvertes.fr/file/index/docid/767404/filename/pairings.pdf

[11] PBC library: The pairing-based cryptography library. http://crypto.stanford.edu/pbc/.

[12] R. A. Popa and N. Zeldovich. Multi-key searchable encryption. Cryptology ePrint Archive, Report 2013/508, Aug. 2013. http://eprint.iacr.org/.

[13] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. 2005a. Hierarchical identity based encryption with constant size ciphertext. In *EUROCRYPT (LNCS)*, Vol. 3494. Springer, 440–456.

[14] Seny Kamara and Charalampos Papamanthou. 2013. Parallel and dynamic searchable symmetric encryption.In *FC*.

[15] Rafail Ostrovsky, William E. Skeith III, "Private Searching On Streaming Data" Journal of Cryptology, Volume 20:4, pp. 397-430, October 2007.

[16] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. 2006. Searchable symmetric encryption: Improved definitions and efficient constructions. In *CCS*. ACM, New York, NY, 79–88. DOI:http:// dx.doi.org/10.1145/1180405.1180417

[17] Philippe Golle, Jessica Staddon, and Brent Waters. 2004. Secure conjunctive keyword search over encrypted data. In *ACNS*. LNCS 3089, 31–45.

[18] Hyun-A Park, Bum Han Kim, Dong Hoon Lee, Yon Dohn Chung, and Justin Zhan. 2007. Secure similarity search. In *GrC*. IEEE, 598–604.

[19] Yanjiang Yang, Haibing Lu, and Jian Weng. 2011. Multi-User private keyword search for cloud computing. In *CloudCom*. IEEE, 264–271.

[20] Giovanni Di Crescenzo and Vishal Saraswat. 2007. Public key encryption with searchable keywords based on jacobi symbols. In *INDOCRYPT (LNCS)*, Vol. 4859. Springer, 282–296.

[21] Adriana Lopez-Alt, Eran Tromer, and Vinod Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In STOC, pages 1219–1234, 2012.

[22] Yanjiang Yang, Haibing Lu, and Jian Weng. Multi-user private keyword search for cloud computing. In CloudCom, pages 264–271, 2011.

[23] Remya Rajan. Efficient and privacy preserving multi user keyword search for cloud storage services. In IJATER, pages 48–51, 2012.

[24] Fangming Zhao, Takashi Nishide, and Kouichi Sakurai. Multi-user keyword search scheme for secure data sharing with fine-grained access control. In ICISC, pages 406–418, 2011