IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

RESULTS OF EXPERIMENTS ON DIFFERENT ELLIPTIC CURVES AND APP LAYOUTS FOR MULTI-KEY SEARCHABLE ENCRYPTION

[1]**Dr Sumaiya Samreen,** Associate Professor,
[2]**Putta Srivani,** Associate Professor
[3]**Sanjeevini Harwalkar** Assistant Professor,
Department of Computer Science & Engineering,
Malla Reddy Engineering College for Women,
Maisammaguda, Hyderabad-500100

ABSTRACT

The multi-Key searchable encryption strategy is a mechanism that may be utilised in order to carry out a keyword search on encrypted text. The server has the ability to carry out operations such as searches on the encrypted data when this approach is used in client-server applications to ensure data secrecy. This method may also be used to keep data private. This research presents the experimental findings of a multi-key searchable encryption system that was created for various different types of elliptic curves. The results of these experiments are compared against one another. a computer software that was constructed with Java serving as the front end and MongoDB acting as the back end. In addition, it shows the period of time that must pass before this method may be utilised to sift through the encrypted data.

Keywords: the phrases "encryption," "search token,"

1. INTRODUCTION

A network called cloud computing provides various computer services, such as servers, databases, storage, and software, on a pay-per-use basis. When using the cloud for data storage, the issue is how information is saved in the cloud and how it is retrieved from the cloud. There is a danger of information leakage when plain text data is allowed to be stored on the cloud. So Data Storage and Information Retrieval is a really difficult problem. Outsourcing solely encrypted data is a potential strategy for achieving confidentiality. In one-user apps, the client only performs encryption and decryption on the client side while the server retains the encrypted data. Every user can access the documents in multi-user apps, which The ability to find encrypted data shared by different users is supported by calendar and assignment submission apps. In the past, search tokens had to be provided by the server by the client under each key of all the documents he had access to for the searchable encryption approaches to work. However, such techniques may operate slowly when the server has to look through a large number of documents.

Due to the multi-key searchable encryption system, the server is able to search all of the documents that are encrypted with various keys using just one token that was supplied by the client [12]. This is possible since the server has access to all of these documents.

Encryption and decryption operations are carried out on the client side under this method. With the help of this approach, the server can look through encrypted data. In this technique, the client merely sends the server a single token that was produced for that search term. This token is used by the server and transformed into a search token for all the files that have been encrypted using various keys. The biggest benefit Only one token of the search term is being transferred to the server in this scheme.

Different search tokens used for various documents are not transmitted. Since the search operation is carried out on encrypted data, it also offers data security.

This system has two difficult problems: it can be used for real-time web applications and there is no reliable third party to distribute the keys through. We outline this scheme's experimental outcomes for various elliptic curve settings. By employing this method, a Java front-end and MongoDB back-end application have been created. We calculated the amount of time needed to search lakh records of encrypted data. This method was used to create various elliptic curves and estimate how long each elliptic curve would take.

2. GENERALMODELOFSEARCHABLEENCRYPTIONMETHOD

Since it is common knowledge that cloud storage is used for data backups, data must be kept in a format that cannot be read. This reduces the likelihood that an individual's privacy will be compromised. In order to carry out the search process, the user will send a query to the server. The documents are decrypted on the server, and a search is conducted using the plain text of the files. When compared to other strategies, this one requires a larger time investment.

Theserver runs the search operation on the cipher text to cut down on the time spent searching. Searchable encryption refers to this query.

USER SERVER
Encrypted files
Upload → Encrypted

TextQuery → Search(cipher

Text)

Fig.1.SearchableEncryptionMethod-AGeneralModel

3. LITERATURE SURVEY ON SEARCHABLEENCRYPTIONSCHEMES

Encryption is the procedure that is utilised in order to keep data confidential. When working with encrypted text, performing a search operation might be challenging. Cloud computing is only one example of the many different searching methods that have been developed in order to carry out the search operation on the encrypted text when the data is outsourced.

The information Retrieval System (IRS) has always offered data users multi-keyword ranked search. The issue of searching on cipher text has been addressed by an algorithm that has been proposed by[1], which uses semantic analysis to perform a search operation for multiple keywords across encrypted material, returning a file that contains the keyword search results.

The single-user settings are the only ones available for all searchable encrypted schemes over encrypted databases. Feng Bao, Robert H. Deng, Xuhua Ding, and Yanjiang Yang[2] have created a system model that provably satisfies a set of security requirements for multiuser searches. According to their proposed architecture, each user is given a unique key; as a result, any authorized cancellation of a user does not necessitate re-encrypting the database or updating the query keys, and it is transparent to users whose authorization has not been withdrawn. Additionally, authorized users can search the database and conduct insertion operations, which is a crucial feature in a multi-user environment where data sharing is required.

Using a mechanism known as a public key system, Dan Boneh, Giovanni, Rafael Ostrovsky, and Guiseppe[3] proposed an idea to execute the search operation on cipher data. Let's say that user Alice wants to send user Bob an email that is encrypted using Bob's public key. For instance, a mail server might check to see if a message contains the keyword "resign." Since the emails are encrypted, the email server is unable to search the data because it is in encrypted form. So they came up with a plan that allows Bob to give the email server a key. Using the key, the server creates a trapdoor for the word and runs the test. The server merely posts the outcomes to Bob whether

Two unique searchable symmetric encryptions have been published by Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky [4]. These encryptions may be utilised in multiuser scenarios that need safe constructions, and they were developed by these researchers.

Eu-Jin Goh [5] developed an efficient and safe index schene that he calls Z-INDEX for the purpose of doing searches on encrypted data. Z-INDEX is constructed utilising Bloom filters and pseudo-random function generators. In addition to that, he explains how to utilise Z-INDEX.These methods can be used to create secure set membership tests, hashing algorithms, private query database systems, and searchable encrypted audit logs.

The Dynamic Searchable Symmetric Encryption system, put up by Seny Kamara, Charalampos Papamanthou, and Tom Roeder [6], permits the removal and inclusion of files from the database. All of these operations are managed by this scheme using tokens. The custom creates an added token that the server will use to update the encrypted index when a file is added. To delete a file, the server uses a delete token that the client generates to remove the encrypted index.

Song Dawn Xiaodong Mr. David Wagner Four cryptographic searchable techniques have been put out by Adrian Perrig[7] so that users can conduct searches on cipher data while preventing the server from receiving plain text. These algorithms offer sequential scanning, controlled searching, and hidden searches.

The system was then created by Goh [5], Chang, and Mitzenmacher [8,] to conduct searches on cipher text indexes that were created for a collection of documents. Their systems increased the search efficiency for big storage with created indexes. The ratio of the total number of keywords to the bit-length generated for each document index is efficient. Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky [4] have developed two unique searchable symmetric encryptions. These encryptions may be employed in multiuser scenarios that need safe constructions, and they were published.

Eu-Jin Goh [5] has developed an efficient and reliable secure index schene that he calls Z-INDEX. This index is constructed via Bloom filters and pseudo-random function generators. Additionally, he details how to put Z-INDEX into action.

Seny Kamara Charalampos Papamanthou[14] designed a system of searchable symmetric encryption (SSE) called Parallel and Dynamic Searchable Symmetric Encryption to enable parallel search. It searches a keyword, "w," in O(r) parallel time, where r specifies the document count. This method also accomplished features like external memory implementation, security from adaptive chosen keyword attacks, etc. This approach is based on the random oracle concept and uses red-black trees, a non-linear data structure.

Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky [4] have developed two unique searchable symmetric encryptions. These encryptions may be utilised in multiuser scenarios that need safe constructions, and they have been published.

Eu-Jin Goh [5] developed an efficient and safe index schene that he calls Z-INDEX for the purpose of doing searches on encrypted data. Z-INDEX is constructed with the use of Bloom filters and pseudo-random function generators. In addition to that, he explains how the Z-INDEX algorithm should be implemented. This plan achieves IND-CKA security and is sub-linear and optimum. A method termed "conjunctive Keyword Search" was invented by Golle et al. [17].allows for the search of several keywords in a single query. an assumption that each page has keyword fields. Using these key fields, the user searches. In the Random Oracle Model, this plan achieves IND1-CKA security.

Two innovative searchable symmetric encryptions have been published by Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky [4]. These encryptions may be utilised in multiuser settings with secure constructions, and they were developed by these four researchers.

Eu-Jin Goh [5] developed an efficient and safe index schene that he calls Z-INDEX for the purpose of doing searches on encrypted data. Z-INDEX is constructed with Bloom filters and pseudo-random function generators. In addition to that, he provides an explanation of how Z-INDEX should be implemented. The concept behind this technique is to compute encryption for each word character by a character before using Hamming Distance to look up related keywords. It is not secure because of what the encryption has done character-wise. As a result, the security of new iterations of this method has been improved. The PKL+-(I, II) algorithms are safer and more effective. These methods make use of generators, exponentiations, one-way functions, and pseudo-random functions (PRF). One hash is required by PKL+-I for each character in a word. For each character in a word, PKL+-II requires a hash and a PRF. To do a search operation, these two versions determine the Hamming Distance between the keyword and the pattern.

An innovative method of keyword, an effective method for encrypting to the future, and forwarding public key secure cryptosystem, are just a few of the many

searches using bilinear mapping in multi-user scenarios developed by Yang et al. [19]. The plan has been created using a bilinear symmetric mapping of prime order. According to Yang et al., by using the user's helper key and trapdoor key to search the index, the server can compute a common key. The bilinear mapping and pairing for each keyword search must be calculated using this approach. Under the two DDH and CDH assumptions of the Random Oracle Model, this technique is demonstrated to be secure.

Crescenzo and Saraswat's concept is to create a MultiWriter technique that will enable search operations to be carried out on encrypted data. They invented a system known as "Public Key

Encryption with Keyword Search by Jacobi symbols." The identity-based encryption proposed by Cock is used in this approach, which is not dependent on bilinear mapping. Its effectiveness has been demonstrated by using 4 million Jacobi symbols, or 160 bits, per keyword to encrypt the data.

The main focus of the research on searchable encryption systems is how searches can be performed while data is encrypted with the same key. Some cryptographic algorithms use public keys, whereas others use secret keys. The only person who has created a searchable encryption system with various keys is the researcher Lopez-Alt et al. [21]. Their system is referred to as "Fully homomorphic encryption." enables the use of any type of operation on encrypted data. By using their keys and the encrypted data, each user can compute a function. Time-consuming, requiring all parties to work together to execute the MPC protocol, and requiring the client to perform some effort to retrieve all the keys are the drawbacks.

These issues are solved by the multi-key searchable encryption system.

Bao et al.[2] conducted yet another study. relates to searching encrypted material where all the papers are encrypted using the same key. Although each user has a unique key in his system, the documents are encrypted using a single key. The limitation of this technique is that it cannot be directly applied to multi-key settings. The multi-user one-key scheme category includes some of the schemes described in [22,23,24] that share characteristics.

One benefit of a multi-key searchable encryption technique is that it may be used in environments with multiple users and multi-key configurations. We can prevent the server from receiving a variety of keys that are used to encrypt various documents.

4. ELEMENTARYCONCEPTONELLIPTICCURVES

4.1 Introduction

The field of integers modulo q, where q is a prime number, is represented by Fq. A finite field (Fq) over an elliptic curve (EC) is represented by an equation.

i2 = j3 + aj + b, where a and b are members of Fq, fulfills the criterion.

(Mod q) 4a3 + 27b2 = 0.

A pair (j, i) is the place on the curve where j, I Fq and the point (j, i) should satisfy the equation. The "point at infinity," also known as the location on the curve, is denoted by the symbol ". The totality of all the points on EC is represented by EC(Fq). The points on the elliptic curve are (0,2), (0,5), (1,0), (2,3), (2,4), (3,3), and (3,4) when the equation i2= j3 + 2j +4 and the elliptic curve EC over F7 are used.

4.2 EllipticCurveKeyGeneration

Give Fq the ability to define the finite field of an elliptic curve EC. Consider the possibility that 'P' is a point in EC(Fq) and that 'P' possesses prime order n. Let's say that the cyclic subgroup that 'P' produces is denoted by EC(Fq).

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

Let q, EC, and P denote the public domain parameters, the prime number, and the elliptic curve equation, respectively.

and the point with order 'n', respectively. Let's be a private key with an integer value chosen uniformly at random from the range [1, n-1]. Q=mP will serve as the equivalent public key.

4.3 Mapping on the Elliptic Curve Using a Bilinear Function

It is possible to establish a mapping that goes from two points on an additive elliptic curve (EC) over a field (n) to a member of a multiplicative group with finite extension (N). It is expressed as the equation e(aC, bD) = e(C, D)ab, where C and D stand for elliptic curve points and a and b are integers. This process is referred to as bilinear mapping (e)[10], and it is stated as the equation.

For cryptographic bilinear mapping, two techniques are used: modified Weil pairing and Tate pairing.

4.4TypesOfEllipticCurves

A curve of type A is an elliptic curve, and its definition is given by the equation y2 = x3 + x.

Let's say that the one that is used to construct the pairings is the Field called "F pq," where "pq" might be any prime number; for instance, pq=3 percent. Let's speak about the group of E(F pq) points that are generated on the elliptic curve by employing the pairings G1 and G2. As a result of this, a combination has arisen that strikes a balance between the two of them. The expressions E(F pq)=pq+1 and E(F pq2)=(pq+1)2 are interchangeable and have the same meaning. The embedding degree is a "2" from that point on. The group GT is a subgroup of the group F pq2, and the order of some prime factor is referred to as "r." This order is indicated by the notation "pq+1."

Curve of the type B: A Type B curve is an elliptic curve that has the equation y2=x3+1 as its defining equation. Let's make the assumption that the field F pq is the one that's used to produce the pairings and that "pq" is a prime integer, with the condition that pq=2 minus 3 in order to simplify things. Calculating cube roots is made easy by the F pq function. If we appropriately restrict 'pq,' we will be able to accomplish it for Type A pairings as well.

The curve of type C: Supersingular curves, or type C curves, have the formulae y2=x3+2x-1 and y2=x3+2x+1. Over a "3" characteristic field, these curves are built. Utilizing well pairing, these curves are used to create brief signatures. By using optimization techniques, we can accelerate the pairings.

The curve of type D: Type D curves are regular curves with the equation y2=x3+ax+b. With a field and order h*r, type D curves are created. 'h' is a small value, and 'r' is referred to be a prime number.

The type E curve satisfies the complex multiplication method-created Diophantine equation DV2=4q-t2. If t=2 and some integers h and r are prime numbers, then q=D r2h2+1. V=2rh can be used to solve this equation. The order q-1 of a type D curve. As you can see, these curves have an embedding degree of 1, and power (r,2) divides q-1. For group elements to be represented, a lot of memory is needed due to the 'q's' 1024-bit capacity. If optimizations are made to Type D curves, slow pairing results.

Curves of type F have the following equations: E: y2= x3+ b.A12-embedding degree allows for the formation of pairings. These curves only require 160 bits to represent the components of one group and can be used to indicate an embedding degree. Short signatures with enhanced security can be created using curves with an embedding degree of 12.

Type G curve: Elliptic curves made using the formula y2=x3+ax+b are referred to as Type G curves made using the complex multiplication approach. The order 'h*r' is used to define these curves.

Supersingular curves, also known as type I curves, have the formula Y2=X3-X+1 with a finite field of F_(3n). For these curves, a '6' Embedding Degree is used. Let G1, and G2 make up the group of points (F_3n), while GT designates a subgroup of F_(3n).

5. SCHEME

Let's get a little more into the specifics of how the Multi-Key Searchable Encryption Scheme works behind the scenes for "n" users. Let's imagine that user I possesses a public key formatted in the puki manner for each user. Let's say that the document key for the user i's document j is denoted by the letter Kj. As an example, let's say Bob has n pieces of paper that are encrypted and stored on the server side using a key kj for each document, where j might vary anywhere from 1 to n. Bob wants to keep the documents as secure as possible. He wants to seek for the letter "w" in all of the documents that he is permitted to access, therefore he will do a search on all of those documents. His public key is utilised in the generation of a token for a search phrase, which is subsequently transmitted to the server when the process has been completed. He sends the server a public data set that is known as the DELTA VALUES that were created for each key 'kj' and.

By using DELTA VALUES, the server modifies the search token that was generated with his public key in order to generate a search token that is lower than kj. This is done in order to provide a search token that is valid. Because this technique makes use of DELTA VALUES in order to carry out a search procedure across all of the documents, the server is in a position to produce search tokens for each and every one of the documents when it is put into action. Because the server is only provided with a single key, this method is particularly useful for carrying out search operations.

Every type of elliptic curve is used to execute the technique in this research, and their performance in terms of time is compared.

6. CONSTRUCTION

The hash functions H 1 : 0,1 G 1 and H 2 : G T X G T 0, 1 are described in this technique as random oracles. These functions are referred to by their respective acronyms. What exactly is meant by the term "Multi-Key Searchable Encryption"? params

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

  The function MKY.Setup(1k) is used to configure the curve's parameters.

- return puk MKY.KeyGen(params): pukZp.
  It is a tool for creating the public key.

- K1←MY.KeyGen(params):returnk1←Zp.

  The 'K1' key is generated using the MY.KeyGen(params) method. This key is used to encrypt the text file.

- Δ← MY.Delta(puk,k1):returnΔ =$g^{k1/puk}$∈G2.

  MY.The function used to create the delta value is called delta (puk, k1). The 'k1' key and public key puk are used to generate delta. The 'delta' is computed by the user and sent to the server.

- tk←MY.Token(puk,w):returntk=H(w)^{puk}∈G 1.
  MKY.The function Token(puk,w) is used to create a token between the keyword "w" and the public key "puk".

- c← MY.Enc(puk,w): Drawr ← GT .Outputc=
  (r,H2(r,e(H(w),g2)^{puk}))
  MY.Enc(puk,w) is a function that the client uses to carry out word encryption.

- tk′←MY.Adjust(tk,Δ):returntk′=e(tk,Δ)∈GT.
  The function MKY.Adjust(tk,) is used to create the search token 'tk'.

- bit←MY.Match(tk,ct):Letct=(r,n).ReturnH2(r,tk)?=n.
  The function MKY.Match(tk, ct) compares the search term with the encrypted text file. If the keyword is located in the file, it returns true; otherwise, it returns false.

7. EXPERIMENTALRESULTS

Different elliptic curves and an are implemented for the Multi-Key Searchable Encryption Scheme.

Table 1 Shows The Multikey Searchable Encryption Algorithm With All Elliptic Curve Types Over Time

Algorithm	Type	Type	Type	Type	Type	Type	Type	Type	Type	Type	Type
hm	A	A1	Dwith159 no.ofbitsin the q	Dwith 201 no.of Bits in the q	Dwith 224 no.of Bits in the q	Dwith 105171-196-185	Dwith 277699-175-167	Dwith 278027-190-181	E	F	G
Time(s	0.041	0.178	0.291	0.048	0.050	0.041	0.037	0.037	0.053	0.094	0.089
)	679	408	05	337	077	106	007	233	924	740	775

8. IMPLEMENTATION

This scheme can be used to design applications for the cloud system, such as messaging apps, home works, big data analytics apps like advertising and marketing, data storage apps that support storing and retrieving of required data, and so on. To perform a sequential search operation on the cypher text using this scheme is possible. Front-end programming is done in Java, while the back-end database is managed using MongoDB. Using a JSON online generator, one million records are generated at random. This app's purpose is to provide an estimation of the time required to do sequential searches on encrypted documents. Three collections have been implemented for this application.

a) A collection titled "Restaurant"

b) The Rest collection

b) collection called delta

a) The plain text documents that are produced at random by comparison between the various elliptic curve implementations are stored in the restaurant collection.

The method was written in the programming language "C" and run on the Ubuntu operating system. It made use of the PBC library[11] and a variety of elliptic curves with different pairing parameters.The testing findings using a twin-core Intel i3 -3120M processor running at 2.50 GHz are shown below.

When implementing the procedure using various

elliptic curves, Type D curve implementation required less time than all other types of curve implementation when using the JSON online generator. There are four columns in this group.
Address, name, and object IDs are all required.
Object_id: The id for each document is kept in this column. In MongoDB, it is implicitly created.
Name: The restaurant names are used in this column.
Address: It's used to hold the restaurant's address.

Restaurant_id: This field is used to hold the restaurant's ID.

To store the encrypted documents, a Rest collection is made. There are three columns: id, name key, and name.

Id: This column is used to record the document's object id. It is generated automatically by MongoDB.

Name key: The encrypted names of the restaurants that are listed in the Restaurant collection's field "name" is kept in this column. The search operation is done in this column.

Name: The names of the eateries are included in this column for verification.

c) The delta values are stored in a delta collection. The search operation makes use of these values. Three columns are present.
"id delta" key

Id: This column is used to record the document's object id. Its values are implicitly generated by MongoDB.

Delta: The values for the delta are kept in this column. Two keys are used to create deltas. i.e., the document's encryption key and the user's public key.

Key: This is a column used to store the encryption keys for documents. The 'name' field in every one of the documents that make up the Restaurant collection has been encrypted using the appropriate key values.

Table 2 presents the results of experiments conducted with a programme developed specifically for the purpose of performing sequential searches on ciphertexts using the aforementioned methodology.

Table 2 Experiment Results Using Dual Core Intel Processor

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

The implementation capability of this technique for sequential searches on encrypted data constitutes a limitation. Additionally, it can be improved to support encrypted data index-based search operations. The system described above was created to search encrypted data. We tested several elliptic curve settings with a multi-key searchable encryption scheme using the PBC library. In comparison to other curves, the experimental results demonstrate that Type D curve parameters took less time or 0.037007 s. This Type 'D' curve scheme was developed in an application that used Java as the front end and MongoDB as the back end, and it was meant to handle one lakh records.

10.FUTURE WORK

The primary goal is to figure out how to search encrypted data. When information is encrypted with the same key, the authors' research led to the development of algorithms that facilitate search operations. In real-time applications, these methods cannot be used in a multi-key environment. Other schemes are included in the category of multi-user one-key schemes. In a multi-user environment where the documents are encrypted with various keys, a multi-key searchable encryption system can be used. This system can yet be improved to support 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

a. 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 an
[5] Efficient Constructions,’’ in Proc. ACM CCS, 2006, pp. 79-88.
[6] E.-J. Goh, ‘‘Secure Indexes,’’ in Cryptology ePrint Archive,2003[Online].Available: http://eprint.iacr.org/2003/216
[7] Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic searchable symmetric encryption. In CCS, pages 965– 976, 2012.
[8] Dawn Xiaodong Song, David Wagner, 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.
[9] 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.
a. D.R. Hankerson, A.J.Menezes and S.A Vanstone, Guide to elliptic curve cryptography. Springer-Verlag, New York 2004.
[10] https://hal.archives-ouvertes.fr/file/index/docid/767404/filename
a. /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.