The Research and Outlook for Keyword-Based Searchable Encryption in Cloud Storage

Liang Hu, Tengfei Li, Yan Li, Jianfeng Chu, Hongtu Li, and Hongying Han
Jilin University, Changchun, 130012, China
Email: {hul, chujf, lihongtu}@jlu.edu.cn; {tengfei13, yanli13, hanhy2112}@mails.jlu.edu.cn

***Abstract*—**In cloud computing, users usually outsource their private data to the cloud storage to save the local storage space and reduce the management costs. Cloud storage is a commonly used cloud computing service which enables users to remotely access data in a cloud anytime and anywhere, using any device, in a pay-as-you-go manner. To protect the confidentiality and privacy of the stored data on the remote untrusted cloud server, cryptographic methods have to be applied. Searchable Encryption (SE) is a recently developed cryptographic primitive that supports keyword search over encrypted data, which enables users to encrypt their sensitive data and store it to the remote server, while retaining the ability to search by keywords. The search process of SE is as follows: A user sends to the server a secret token, the token could be a transformation of the queried keywords; then the server searches the encrypted data according to the token and returns the matched documents. The main purpose of this paper is to research the SE based on keywords in cloud storage. Firstly, we introduce the research background and the current development of SE schemes. Then, we review and make comparison of some related SE schemes. Finally, some issues that need to solve are list.

***Index Terms*—**Cloud computing, cloud storage, keyword, searchable encryption

I. Introduction

Cloud computing [1] is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet). Clouds can be classified as public, private or hybrid. With the rapid development of cloud computing, some cloud services are access to a wide range of applications, in which cloud-based storage service is one of the most promising applications. The network storage tool Dropbox, Amazon simple storage service, Windows Azure are examples of such commonly used cloud storage services.

Cloud storage services, including database-like services and network attached storage, are often billed on a utility computing basis. Cloud storage services enable users to remotely access data in a cloud anytime and anywhere, using any device, in pay-as-you-go manner. [2] By moving their data to the cloud, users can avoid the costs of building and maintaining private storage infrastructure, opting instead to pay a service provider as a function of its need. [3] Cloud storage is used by a large number of individuals and enterprises. All data stored on their hard drive is not cared by user and no one knows where exactly data saved. Most of the data will be stored in a network computing system on top of the cloud, data security and user privacy have become of great concern to the user. [4] Thus, security and privacy issues in terms of the Cloud Service Provider (CSP) as well as the potential illegal users are receiving an increased amount of attention in the literature.

To ensure the confidentiality of data, cryptographic techniques are commonly used, more and more individuals and enterprises encrypt their data before storage and the data is stored in cloud server in the form of ciphertext. However, in this context, when a user wants to search a file which contains certain keywords, how to search the ciphertext is a problem. The existing access control schemes and authentication schemes can solve this problem to a certain extent, while these schemes depend mainly on users' complete trust to CSP. To solve this problem, one of the simplest methods is to download all ciphertexts and decrypt them [5], then search the plaintexts based on keywords. However, this method is not practical. Since most data downloaded are unneeded, it wastes a lot of network overhead and storage overhead; Moreover, at the same time, it depletes too much CPU capability and memory power of the client during the encryption and decryption. Therefore, this scheme cannot work well under these circumstances. Another method is to send the key and keywords to cloud server, CSP decrypts the ciphertexts and searches, then return the matchable data. While with such a method, a customer's privacy information as well as some important business secrets are exposed to the CSP, even worse, an untrustworthy CSP is able to easily obtain all the information, thus brings great security risks.

Searchable Encryption (SE) technique provides a solution to such problem. It enables the users to encrypt their sensitive data and store it to the remote server, while retaining the ability to search by keywords. While searching, the user sends to the server a secret token, the token could be a transformation of the queried keywords; then the server searches the encrypted data according to the token and returns the matched documents. During this

Manuscript received March 9, 2015; revised September 21, 2015.
This work was supported by the Deep exploration instrumentation and equipment development (SinoProbe-09-01-03) under Grant No.201011078
Corresponding author email: chujf@jlu.edu.cn.
doi:10.12720/jcm.10.10.766-772

process, the server does not know what the queried keywords and the document contents are, and therefore the privacy is guaranteed. [6] The architecture of cloud storage is as Fig. 1. With SE method, the CSP to determine whether a given file contains certain keywords specified by a user, but is not aware of any information about both the keywords and the file. In terms of access efficiency, SE method makes the search process more convenient. Firstly, Users needn't waste the transmission overhead and storage space for the files that don't contain the corresponding keywords; Secondly, SE method enables CSPs to participate in the partial decipherment so as to reduce computational overhead on users, without leaking any information about the plaintext and the submitted keywords; Thirdly, the decryption overhead of redundant files can be saved.

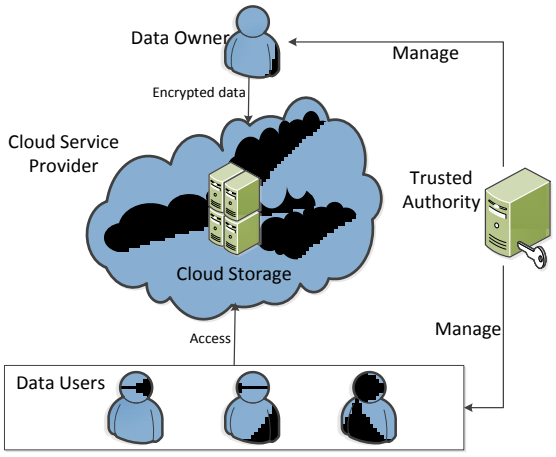


Fig. 1. Architecture of a cloud storage system.

This paper is focus on the cryptographic solutions to protect the confidentiality and privacy of the stored data on the remote untrusted cloud server. SE is one of the mostly used such solutions. The paper is structured as follows: Firstly, we conclude the related work and some existing typical schemes in Section II, and analysis the security and efficiency of the existing schemes in Section III. Then, we present some unsolved issues and the future work of searchable encryption in cloud storage in Section IV. Finally, we conclude this paper in Section V.

II. Related Work

In this section, we illustrate the previously proposed cryptographic approaches which are used to protect privacy of outsourced data. There are many types of SE schemes, each of which corresponding to some particular application scenarios. Basic SE schemes could be divided into two approaches, which are Private Information Retrieval (PIR) [7] and SE. Researches on SE can be further classified into two categories, which are symmetric key cryptography based SE (SSE) and public key cryptography based SE (PSE). There are two main differences between SSE and PSE: Firstly, since most PSE schemes are built on the basis of bilinear mapping, the calculations between group elements and bilinear pairings are needed in the search process. Therefore, the computing overhead in PSE is usually much larger than in SSE; Secondly, SSE schemes are more applicable for those scenarios that one single user create documents and share them with multiple users. While PSE mechanism allows not only the data owner, but also other users who have the public key to generate ciphertexts data and share them.

A. PIR

In cryptography, a PIR protocol allows a user to retrieve an item from a server in possession of a server without revealing which item is retrieved. PIR is a weaker version of 1-out-of-n oblivious transfer, where it is also required that the user should not get information about other document items.

PIR uses cryptographic tools to ensure hiding the keyword search and the result of the query from the adversary server while retrieving the most relevant data to the user. In this approach, it enables a user to access k ($k \geq 2$) replicated copies of a server and privately retrieve information stored in the server. [7] Server holds N elements. User is interesting to retrieve a certain element without disclosing to the server which data element is retrieved [8], [9].

PIR is always working with unencrypted data. Such feature requires from PIR to touch all the stored data to protect the retrieved data (access pattern). Otherwise, the adversary server learns that the untouched data are not interested to the user. Such inefficient scheme is not practical especially in case of large scale cloud computing. Many papers are presented to improve the efficiency of PIR, such as [10], [11]. However, PIR schemes are designed in order to achieve higher security than we require (in a computational sense, the server in a PIR scheme has no information about what documents are retrieved) and thus come with far higher communication cost.

To gain better efficiency, SE schemes are used to hide the queried keywords and the stored data instead of hiding which data is retrieved.

B. SSE

Symmetric-key algorithms [12] are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The main advantage of symmetric key algorithms is its small computing overhead. The disadvantage is the issues of key negotiation. The encryption key and decryption key must be negotiated in advance, so secure channel for key transmission is necessary.

SSE allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. Such schemes are constructed with pseudorandom function generator, pseudorandom number generator, Hash algorithm and

symmetry encryption algorithms. When search the documents based on keywords, the keywords are processed randomly, then the server match the keywords by preset method. T

Most SSE systems employ the block cipher and hash function methods to encrypt their data. The first practical SSE is proposed by Song *et al*. in [13] in 2000. In this scheme described as Fig. 2, each word within the document is encrypted with a two-layer encryption scheme. With this scheme, the untrusted server cannot search for an arbitrary word without the user's authorization and the user may ask the untrusted server to search for a secret word without revealing the word to the server. However the presented scheme does not use the searchable index structure, instead they use the sequential scan, which makes the search time liner to the underlying encrypted data. Moreover, it leaks the position of the searched keywords to the adversary server. Later, Goh proposed a data structure called secure index [14] that allows query with a "trapdoor" for a word, every index is dedicated to each document in the collection. The client indexes and encrypts its document collection and sends the secure index together with the encrypted data to the server.

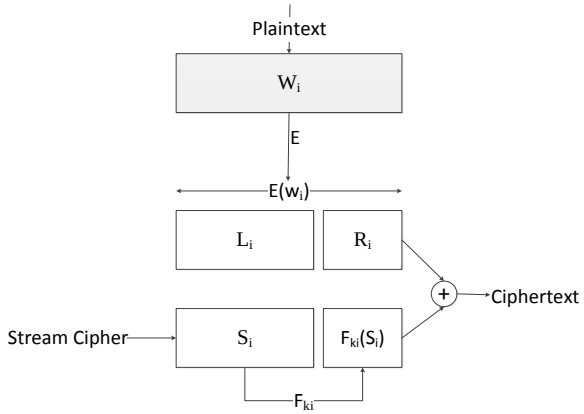


Fig. 2. Final scheme in Ref. [13]

By using the SSE techniques [15], any type of search query can be achieved without leaking any information to the server, not even the "access pattern", such as SSE in this multi-user setting [16], conjunctive keywords based searches over symmetrically encrypted data [17], [18], multi-keyword ranked search over encrypted data [19]. This strong privacy guarantee, however, comes at the cost of a logarithmic (in the number of documents) number of rounds of interaction for each read and write. Hereafter, with the development of cloud computing, keywords searches over encrypted data based on SSE are extended to cloud computing environment [18]-[20].

C. PSE

The current existing PSE schemes are constructed on basis of bilinear pairing. The security of PSE is usually built on the intractability of complex problems. In a PSE scheme, there are two types of secret keys: public key and private key. A data owner builds his index and encrypts it with the public key and uploads it together with the encrypted documents to the remote server. Any user who has gained the public key can insert his data into the stored index. Only those who have gained corresponding private keys are able to perform the search operation. However, most existing PSE schemes suffer from the lack of efficiency as they depend on relatively slow operations like pairing operations on elliptic curves.

Brent, Water *et al*. implement an audit log for database queries [16] that uses hash chains for integrity protection and identity based with extracted keywords to enable searching on encrypted log, which has been widely used beyond searchable audit logs. In 2004, Boneh *et al*. proposed a Public Key Encryption with Keyword Search (PEKS) scheme [21], [22]. This PSE scheme is built on Identity Based Encryption (IBE) in email environment [23]. It enables a gateway to test whether certain keywords are contained in an email without learning any information about the email and keywords. The key technique to make the PEKS scheme work is that an email, corresponding keywords are encrypted under the standard public key encryption algorithm and the PEKS algorithm, respectively. However, with PEKS scheme, the verifier can merely use an untrusted server, which makes this notion very practical. PEKS provides guidance for later researches to achieve more diverse PSE schemes. Hereafter, a lot of improved schemes have been successively proposed. In [24], Golle *et al*. defined two protocols for conjunctive keyword search over encrypted data, for which for which it is provably hard for the server to distinguish between the encrypted keywords of documents of its own choosing. The protocols allow secure conjunctive search with small capabilities. Yong Ho Hwang *et al*. study the problem of a Public Key Encryption with Conjunctive Keyword search (PECK) and further extend PECK to multi-user environment, which called a multi-user PECK. [25] A multi-user PECK scheme can achieve an efficient computation and communication overhead and effectively manage the storage in a server for a number of users. After that, multi-user PSE has been widely studied [26]. Ming Li *et al*. established a scalable framework for Authorized Private Keyword Search (APKS) [27] over encrypted cloud data, which enables efficient multi-dimensional keyword searches with range query, allows delegation and revocation of search capabilities. Moreover, it enhances the query privacy which hides users' query keywords against the server.

The APKS schemes proposed in [27] are based on a recent cryptographic primitive, Hierarchical Predicate Encryption (HPE) [28]. In [29], Jonathan *et al*. constructed predicate encryption schemes. This scheme enables constructions in which predicates correspond to the evaluation of disjunctions, polynomials, CNF/DNF formulae, or threshold predicates (among others). However, the computational overhead is 50 times larger than a Prime order [30]. In addition, [31] considered a new notion called predicate privacy and constructed a cryptographic primitive that tokens reveal no information

about the encoded query predicate. The notion of predicate encryption (PE) was explicitly presented by Katz, Sahai and Waters [20] as a generalized (fine-grained) notion of encryption that covers identity-based encryption (IBE) [32] , [33], Hidden-Vector Encryption (HVE) [34] and Attribute-Based Encryption (ABE) [35], [36]. In a PE scheme, Informally, secret keys in a predicate encryption scheme correspond to predicates in some class *F*, and a sender associates a ciphertext with an attribute in a set $\mathbf{\Sigma}$; a ciphertext associated with the attribute $I \in \mathbf{\Sigma}$ can be decrypted by secret key SK_f to the predicate $f \in \mathbf{F}$ if and only if $f(I) = 1$. [28] PE can be applied to ciphertext searching, in which the attributes of every ciphertext characterized by the typical keywords included in corresponding document, predicate can be seen as the query statement, the private key can be regarded as the search token. If $f(I) = 1$, it presents that keywords of the ciphertext satisfy user's query.

III. Security and Efficiency Analysis of the Existed SE Schemes

A. Preliminary

Definition 1: Bilinear map

Let $\mathbf{G_1}$, $\mathbf{G_2}$ and $\mathbf{G_T}$ be three cyclic groups of some large prime order *q*, we view $\mathbf{G_1}$ as an additive group and $\mathbf{G_2}$ as a multiplicative group. We call $e: \mathbf{G_1} \times \mathbf{G_2} \rightarrow \mathbf{G_T}$ a bilinear map if it is a map with the following properties:

- Computable: There is a polynomial time algorithm to compute $e(g, h) \in \mathbf{G_2}$, for any $g, h \in \mathbf{G_1}$.
- Bilinear: $e(g^x, h^y)=e(g, h)^{xy}$ for all $g, h \in \mathbf{G_1}$ and all $x, y \in \mathbf{Z_q}$.
- Non-degenerate: if *g* is a generator of $\mathbf{G_1}$, then *h* is a generator of $\mathbf{G_2}$.

B. SE Mechanism

The current existing SE schemes are various, the definition and used algorithms are different from each other. A general framework of public key encryption based SE scheme mainly includes four algorithms: Setup, Encrypt, GenToken and Query [5].

Setup: This algorithm is executed by authority or data owner and output related secret key. In a SSE scheme, it outputs some secret key such as the key of pseudo-random function. For PSE scheme, a probabilistic algorithm that takes a security parameter as input and outputs a public key *PK* and secret key *SK*.

Encrypt: This algorithm is executed by data owner. With this algorithm, a data owner selects corresponding keywords set from the document content. Then it takes as input a secret key and the description of the keywords set, outputs an index table. In a SSE system, a data owner encrypts the data and keywords set by a symmetric encryption algorithm or a key-based hash algorithm. And in a PSE system, a data owner encrypts them with the Public Key (*PK*).

GenToken: The executor of this algorithm could be a data owner, the authority or a user. It is determined by the application scenario. It takes as input a secret key and the description of keywords from users, and outputs a searchable token.

Query: This algorithm is executed by the storage server. It takes the received searchable token and index table as input in ciphertext form. Then compute them according to the preset algorithm, and output a message by comparing the computing result with the preset result. If the preset result is satisfied, the search result and corresponding content can be returned to the user. Otherwise, the content cannot be returned.

At last, once a user receives the requested content, he could decrypt the ciphertext with corresponding secret key. In a SSE system, the secret key is the symmetric key. And in a PSE system, the secret key is the secret key SK corresponds to this user.

C. Search Results Analysis

With the development and of SE, flexible search result is becoming more and more significant for effective SE schemes. It makes users describe their willingness more realistic and accurate, so that it could targeted to files which are needed. SE schemes could be classified into three categories, which are Single keyword search, Conjunctive multi-keyword search and Complex logic structures multi-keyword search. Table I lists several commonly used SE schemes and the search mode they support.

TABLE I. COMPARISON OF SE SCHEMES

Schemes	Search Support	Algorithm Based
SWP00[13]	Single	SSE
BKM05[17]	Conjunctive	SSE
PEKS[21]	Single	PSE
PECK[25]	Conjunctive	PSE
GSW04[24]	Conjunctive	PSE
HPE[28]	Complex	PSE

D. Security Analysis

The security guarantees provided by SSE are, roughly speaking, the following [3]:

1. Without any tokens the server learns nothing about the data except its length.

2. Given a token for a keyword w, the server learns which (encrypted) documents contain w without learning w.

While these security guarantees are stronger than the ones provided by both PSE, we stress that they do have their limitations. In addition to the issues outlined above, all currently known constructions have deterministic tokens which essentially means that the service provider can tell if a query is repeated (though it won't know what the query is). [3]

The security guarantees provided by PSE are, roughly speaking, the following [3]:

1. Without any tokens the server learns nothing about the data except its length.

2. Given a token for a keyword w, the server learns which (encrypted) documents contain w.

Notice that 2. here is weaker than in the SSE setting. In fact, as pointed out by Byun *et al*. [37], when using a PSE scheme, the server can mount a dictionary attack against the token and figure out which keyword the client is searching for. It can then use the token (for which it now knows the underlying keyword) and do a search to figure out which documents contain the (known) keyword.

IV. Future Work

The research on SE has been for years, while there are still a lot of problems to be solved.

1. The research on search with a single keyword and "AND" search with multi-keywords over encrypted data have obtained several achievement. The efficient search of phrase and sentence is an important issue to be solved.
2. Most of the proposed SE schemes only allow a user to search over encrypted data through exact keywords. That is to say, there is no tolerance of minor typos and format inconsistencies which are typical user searching behavior and happen frequently. This significant drawback makes existing techniques unsuitable in cloud storage environment. Some fuzzy keywords SE schemes have been proposed [38], while there are great necessities to further improve the proposed schemes and seek for more efficient schemes.
3. Some existing SE schemes could support the range query and subset query. While the support of relational operation is still unsatisfactory, in which the relational operation is based on ">", "<", "==" and so on. Research in this area is currently a hot topic.
4. Most schemes are not work well in cloud storage environment. Frequent decryption will deplete too much CPU and memory capabilities of the client and lose the critical virtue of cloud computing, i.e., enabling users to access data in a cloud anytime and anywhere, using any device. [22] Therefore, the efficiency must be further improved in the future work to practically apply the SE technology to cloud storage.
5. The research on SE mechanism is mainly focus on the theoretical study. Due to the high complexity etc., it is difficult to be widely used in practice. With the development of cloud computing, the efficiency of SE schemes must be improved gradually to be applied into practice.

V. Conclusion

In this paper, we make a comprehensive presentation and discussion of SE mechanism as well as the application of SE in cloud storage environment. A SE scheme provides a way to encrypt a search index so that its contents are hidden except to a party that is given appropriate tokens. More precisely, consider a search index generated over a collection of files (this could be a full-text index or just a keyword index). Using a searchable encryption scheme, the index is encrypted in such a way that given a token for a keyword one can retrieve pointers to the encrypted files that contain the keyword; and without a token the contents of the index are hidden. In addition, the tokens can only be generated with knowledge of a secret key and the retrieval procedure reveals nothing about the files or the keywords except that the files contain a keyword in common. [3]

Firstly, we introduce the concept of SE as well as its application in cloud storage. Then we conclude the currently existing related works of SE. Next, we present the preliminary about SE in cloud storage, including related definitions, SE application model. Then, we outline a specific algorithm of PEKS. Finally, we conclude some unsolved issues which need further study.

References

[1] P. Mell and T. Grance, "Special publication 800-145: The NIST definition of cloud computing," *National Institute of Standards and Technology*, September 2011.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599-616, June 2009.

[3] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*, R. Sion, R. Curtmola *et al.*, Ed., Berlin Heidelberg: Springer-Verlag, 2010, pp. 136-149.

[4] X. Zhang, H. T. Du, J. Q. Chen, Y. Lin, and L. J. Zeng, "Ensure data security in cloud storage," in *Proc. International Conference on Network Computing and Information Security*, Guilin, 2011, pp. 284-287.

[5] Z. R. Shen, W. Xue, and J. W. Shu, "Survey on the research and development of searchable encryption schemes," *Journal of Software*, vol. 25, no. 4, pp. 880-895, January 2014.

[6] G. C. Luo, N. D. Peng, K. Qin, and A. G. Chen, "A layered searchable encryption scheme with functional components independent of encryption methods," *The Scientific World Journal*, vol. 2014, pp. 16, February 2014.

[7] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *Journal of ACM*, vol. 45, no. 6, pp. 965-981, November 1998.

[8] E. Kushilevitz and R. Ostrovsky, "One-way trapdoor permutations are sufficient for non-trivial single-server private information retrieval," in *Proc. 19th International Conference on Theory and Application of Cryptographic Techniques*, Bruges, 2000, pp. 104-121.

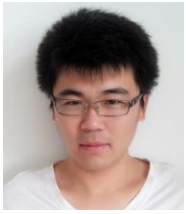
[9] R. Sion and B. Carbunar, "On the computational practicality of private information retrieval," in *Proc. Networks and Distributed Systems Security Symposium Stony Brook Network*, San Diego, 2007.

[10] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Batch codes and their applications," in *Proc. 36th ACM Symposium on Theory of Computing*, New York, 2004, pp. 262-271

[11] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Cryptography from anonymity," in *Proc. 47th Annual IEEE Symposium on Foundations of Computer Science*, Berkeley, 2006, pp. 239-248.

[12] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, Berlin, Heidelberg: Springer-Verlag, 2002, pp. 11-22.
[13] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symposium on Security and Privacy*, Berkeley, 2000, pp. 44-55.
[14] E. J. Goh, "Secure indexes," Technical Report, Stanford University, October 2003.
[15] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," *Journal of Computer Security*, vol. 19, no. 5, pp. 79-88, 2011.
[16] B. Waters, D. Balfanz, G. Durfee, and D. Smetters, "Building an encrypted and searchable audit log," in *Proc. 11th Annual Network and Distributed System Security Symp*, San Diego, 2004.
[17] J. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in *Proc. 7th Int'l Conf. on Information and Communications Security*, Beijing, 2005, pp. 414-426.
[18] J. Li, Q. Wang, C. Wang, M. Cao, K. Ren, and W. J. Lou, "Fuzzy keyword search over encrypted data in cloud computing," *Infocom*, vol. 2009, no. 2, pp. 1-5, 2010.
[19] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Trans. on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 829-837, January 2014.
[20] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in *Proc. IEEE Int'l Conf. on Distributed Computing Systems*, Minneapolis, 2011, pp. 393-402.
[21] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," *Lecture Notes in Computer Science*, vol. 49, no. 16, pp. 506-522, 2003.
[22] Q. Liu, G. J. Wang, and J. Wu, "Secure and privacy preserving keyword searching for cloud storage services," *Journal Network and Computer Applications*, vol. 35, no. 3, pp. 927-933, May 2012.
[23] A. Shamir, "Identity-based cryptosystems and signature schemes," *Lecture Notes in Computer Science*, vol. 21, no. 2, pp. 47-53, February 1985.
[24] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in *Proc. 2nd Int'l Conf. on Applied Cryptography and Network Security*, Yellow Mountain, 2004. pp. 31-45.
[25] Y. Hwang and P. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in *Proc. Int'l Conf. on Pairing-Based Cryptography*, Tokyo, 2007. pp. 2-22.
[26] F. Bao, R. Deng, X. Ding, and Y. Yang, "Private query on encrypted data in multi-user settings," in *Proc. 4th Int'l Conf. on Information Security Practice and Experience*, Sydney, 2008, pp. 71-85.
[27] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *Proc. IEEE Int'l Conf. on Distributed Computing Systems*, Minneapolis, 2011, pp. 383-392.
[28] T. Okamoto and W. Takashima, "Hierarchical predicate encryption for inner-products," in *Proc. 15th International Conference on the Theory and Application of Cryptology and Information Security*, Tokyo, 2009, pp. 214-231.
[29] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Proc. 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Istanbul, 2008, pp. 146-162.
[30] D. Reeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in *Proc. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, French Riviera, 2010, pp. 44-61.
[31] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in *Proc. 6th Theory of Cryptography Conference on Theory of Cryptography*, San Francisco, 2009, pp. 457-473.
[32] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. International Cryptology Conference*, Santa Barbara, 2001, pp. 213-229.
[33] J. Horwitz and B. Lynn, "Towards hierarchical identity-based encryption," in *Proc. Advances in Cryptology-EUROCRYPT*, 2002, pp. 466-481.
[34] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th Conference on Theory of Cryptography*, Amsterdam, 2007, pp. 535-554.
[35] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conference on Computer and Communication Security*, New York, 2006, pp. 89-98.
[36] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symposium on Security and Privacy*, Berkeley, 2007, pp. 321-334.
[37] J. W. Byun, H. S. Rhee, H. A. Park, and D. H. Lee, "Off-line keyword guessing attacks on recent keyword search schemes over encrypted data," in *Secure Data Management*, W. Jonker and M. Petkovic, Eds., Berlin Heidelberg: Springer-Verlag, 2006, pp. 75-83.
[38] J. F. Wang, H. Ma, Q. Tang, J. Li, H. Zhu, S. Ma, and X. F. Chen, "Efficient verifiable fuzzy keyword search over encrypted data in cloud computing," *Computer Science and Information Systems*, vol. 10, no. 2, pp. 667-684, 2013.

Liang Hu was born in 1968. He received the B.S. degree from the Harbin Institute of Technology (HIT), Ha'erbin, and the M.S. and Ph.D. degrees both from the College of Computer Science and Technology, Jilin University (JLU), Changchun. His research interests include Distributed Computing, Network Computing and Security, Data security and privacy and so on.



Tengfei Li was born in 1990. He received the B.S. degree from the College of Software Engineering, Jilin University (JLU) and is currently pursuing the M.S. degree from the College of Software, Jilin University. His research interests include Security of Cloud Storage, Cryptography and so on.

Yan Li was born in 1990. She received the B.S. degree from the College of Software Engineering, Jilin University (JLU) and is currently pursuing the M.S. degree from the College of Software, Jilin University. His research interests include Data Privacy Protection, Cryptography and so on.

Jianfeng Chu was born in 1978. He received the M.S. and Ph.D. degrees both from the College of Computer Science and Technology, Jilin University (JLU), Changchun. His research interests include Network Computing and Security, Data security and privacy and so on.

Hongtu Li was born in 1984. He received the Ph.D. degrees from the College of Computer Science and Technology, Jilin University (JLU), Changchun, China, in 2012. He has been a lecturer with the School of Jilin University since 2012. His current research interests include Network Security, Cryptography and so on.

Hongying Han was born in 1993. She is currently pursuing the B.S. degree from the College of Computer Science and Technology, Jilin University.