International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 10th Febraury 2018. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-02

Title: Dual-server Public-key Encryption through Keyword Search for Sheltered Cloud Storage.

Volume 07, Issue 02, Page No: 175 – 179.

Paper Authors

***CH.LOKESH KIRAN, M.SARADA.**

* Eswar College of Engineering.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DUAL-SERVER PUBLIC-KEY ENCRYPTION THROUGH KEYWORD SEARCH FOR SHELTERED CLOUD STORAGE

***CH.LOKESH KIRAN, **M.SARADA**
*PG Student, Eswar College of Engineering, Narasaraopet, Guntur, AP, India.
**Assistant Professor, Eswar College of Engineering, Narasaraopet, Guntur, AP, India.

ABSTRACT:
Searchable encryption is of increasing interest for protecting the data privacy in secure searchable cloud storage. In thiswork, we investigate the security of a well-known cryptographic primitive, namely Public Key Encryption with Keyword Search (PEKS)which is very useful in many applications of cloud storage. Unfortunately, it has been shown that the traditional PEKS frameworksuffers from an inherent insecurity called inside Keyword Guessing Attack (KGA) launched by the malicious server. To address thissecurity vulnerability, we propose a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS).As another main contribution, we define a new variant of the Smooth Projective Hash Functions (SPHFs) referred to as linear andhomomorphic SPHF (LH-SPHF). We then show a generic construction of secure DS-PEKS from LH-SPHF. To illustrate the feasibility of our new framework, we provide an efficient instantiation of the general framework from a DDH-based LH-SPHF and show that it canachieve the strong security against inside KGA.

Key words-Cloud storage, Encryption, Keyword search, Hash function, Diffie-Hellman language

.1 INTRODUCTION

Cloud storage outsourcing has become a popular applicationfor enterprises and organizations to reducethe burden of maintaining big data in recent years. However,in reality, end users may not entirely trust the cloudstorage servers and may prefer to encrypt their data before uploading them to the cloud server in order to protect thedata privacy. This usually makes the data utilization moredifficult than the traditional storage where data is kept inthe absence of encryption. One of the typical solutions isthe searchable encryption which allows the user to retrievethe encrypted documents that contain the user-specifiedkeywords, where given the keyword trapdoor, the servercan find the data required by the user without decryption.Searchable encryption can be realized in either symmetricor asymmetric encryption setting. In [2], Song et al. proposed keyword search on ciphertext, known as Searchable symmetric Encryption (SSE) and afterwards severalSSE schemes [3], [4] were designed for improvements. AlthoughSSE schemes enjoy high efficiency, they suffer fromcomplicated secret key distribution. Precisely, users have to securely share secret keys which are used for data encryption.Otherwise they are not able to share the encrypted dataoutsourced to the cloud. To resolve this problem, Boneh etal. [5] introduced a more flexible primitive, namely Public Key Encryption with Keyword Search (PEKS) that enables auser to search encrypted data in the asymmetric encryptionsetting. In a PEKS system, using the receiver's public key,the sender attaches some encrypted keywords (referred toas PEKS ciphertexts) with the encrypted data. The receiverthen sends the trapdoor of a to-be-searched keyword to the server for data searching. Given the trapdoor and thePEKS ciphertext, the server can test

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

whether the keyword underlying the PEKS ciphertxt is equal to the one selected bythe receiver. If so, the server sends the matching encrypted data to the receiver.

Related Work

In this subsection, we describe a classification of PEKSschemes based on their security.

Traditional PEKS. Following Boneh et al.'s seminal work[5], Abdalla et al. [8] formalized anonymous IBE (AIBE) and
presented a generic construction of searchable encryptionfrom AIBE. They also showed how to transfer a hierarchical
IBE (HIBE) scheme into a public key encryption with temporarykeyword search (PETKS) where the trapdoor is onlyvalid in a specific time interval. Waters [7] showed that thePEKS schemes based on bilinear map could be applied tobuild encrypted and searchable auditing logs. In order toconstruct a PEKS secure in the standard model, Khader [9]proposed a scheme based on the k-resilient IBE and alsogave a construction supporting multiple-keyword search.

The first PEKS scheme without pairings was introduced byDi Crescenzo and Saraswat [11]. The construction is derived
from Cock's IBE scheme [12] which is not very practical.

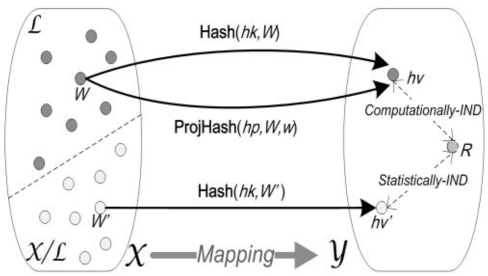
Secure Channel Free PEKS. The original PEKS scheme[5] requires a secure channel to transmit the trapdoors. To
overcome this limitation, Baek et al. [13] proposed a newPEKS scheme without requiring a secure channel, which
is referred to as a secure channel-free PEKS (SCF-PEKS).The idea is to add the server's public/private key pair into
a PEKS system. The keyword ciphertext and trapdoor aregenerated using the server's public key and hence only the
server (designated tester) is able to perform the search. Rheeet al. [14] later enhanced Baek et al.'s security model [13]
for SCF-PEKS where the attacker is allowed to obtain therelationship between the non-challenge ciphertexts and the
trapdoor. They also presented an SCF-PEKS scheme secureunder the enhanced security model in the random oracle
model. Another extension on SCF-PEKS is by Emura et al.

[15]. They enhanced the security model by introducing theadaptively secure SCF-PEKS, wherein an adversary is allowed
to issue test queries adaptively.

Against Outside KGA. Byun et al. [16] introduced the offlinekeyword guessing attack against PEKS as keywords
are chosen from a much smaller space than passwordsand users usually use well-known keywords for searching
documents. They also pointed out that the scheme proposedin Boneh et al. [5] was susceptible to keyword guessing
attack. Inspired by the work of Byun et al. [16], Yau et al.[17] demonstrated that outside adversaries that capture the
trapdoors sent in a public channel can reveal the encryptedkeywords through off-line keyword guessing attacks and
they also showed off-line keyword guessing attacks againstthe (SCF-)PEKS schemes in [13], [18]. The first PEKS schemesecure against outside keyword guessing attacks was proposedby Rhee et al. [19]. In [20], the notion of trapdoor
indistinguishability was proposed and the authors showedthat trapdoor indistinguishability is a sufficient conditionfor preventing outside keyword-guessing attacks. Fang et al.[21] proposed a concrete SCF-PEKS scheme with (outside)KGA resilience. Similar to the work in [15], they also considered
the adaptive test oracle in their proposed security definition.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

SYSTEM MODEL



As illustrated in Fig. 4, an SPHF is defined based on a domain

X and an NP language L, where L contains a subsetof the elements of the domain X, i.e., L _ X. Formally, anSPHF system over a language L _ X, onto a set Y, is definedby the following five algorithms (SPHFSetup; HashKG,ProjKG; Hash; ProjHash):_ SPHFSetup(1_): generates the global parametersparam and the description of an NP language instance

L;_ HashKG(L; param): generates a hashing key hk for L;_ ProjKG(hk; (L; param)): derives the projection key hp

from the hashing key hk;_ Hash(hk; (L; param);W): outputs the hash valuehv 2 Y for the word W from the hashing key hk;

_ ProjHash(hp; (L; param);W;w): outputs the hashvalue hv0 2 Y for the word W from the projectionkey hp and the witness w for the fact that W 2 L.Fig. 4. Smooth Projective Hash FunctionThe correctness of an SPHF requires that for a word W 2

L with w the witness,Hash(hk; (L; param);W) = ProjHash(hp; (L; param);W;w):Another property of SPHFs is smoothness, which means that

for any W 2 XnL, the following two distributions arestatistically indistinguishable :V1 = f(L; param;W; hp; hv)jhv = Hash(hk; (L; param);W)g;

V2 = f(L; param;W; hp; hv)jhv $

Yg;In summary, an SPHF has the property that the projectionkey uniquely determines the hash value of any word in the language L but gives almost no information about thehash value for any point in X n L.In this paper, we require another important property ofsmooth projective hash functions that was introduced in [6].Precisely, we require the SPHF to be pseudo-random. That is,if a word W 2 L, then without the corresponding witnessw, the distribution of the hash output is computationally indistinguishable from a uniform distribution in the view of any polynomial-time adversary. In this section, we first give a comparison between existing schemes and our scheme in terms of computation, size andsecurity. We then evaluate its performance in experiments.

Computation Costs. As shown in Table 1, all the existingschemes [5], [10], [20] require the pairing computation during

the generation of PEKS ciphertext and testing and henceare less efficient than our scheme, which does not need anypairing computation. In our scheme, the computation costof PEKS generation, trapdoor generation and testing are4ExpG1+1HashG1+2MulG1 , 4ExpG1

+1HashG1+2MulG1 , and7ExpG1+3MulG1 respectively, where ExpG1denotes the computationof one exponentiation in G1, MulG1 denotes thecosts of one multiplication in G1, MulG1 and HashG1 respectivelydenote the cost of one multiplication and one hashing operation in G1.

In this paper, we proposed a new framework, named Dual-

Server Public Key Encryption with Keyword Search (DSPEKS),that can prevent the inside keyword guessing attackwhich is an inherent vulnerability of the traditional PEKS

framework. We also introduced a new Smooth ProjectiveHash Function (SPHF) and used it to construct a generic DSPEKS scheme. An efficient instantiation of the new SPHFbased on the Diffie-Hellman problem is also presented inthe paper, which gives an efficient DS-PEKS scheme withoutpairings

REFERENCES

[1] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "A new general framework for secure public key encryption with keyword search," in Information Security and Privacy - 20th Australasian Conference, ACISP, 2015, pp. 59–76..

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order-preserving encryption for numeric data," in Proceedings of the ACM SIGMOD International Conference on Management of Data, 2004, pp. 563–574.

[4] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, 2006, pp. 79–88.

[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in EUROCRYPT, 2004, pp. 506–522.

[6] R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," in EUROCRYPT, 2003, pp. 524–543.

[7] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in NDSS, 2004.

[8] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in CRYPTO, 2005, pp. 205–222.

[9] D. Khader, "Public key encryption with keyword search based on k-resilient IBE," in Computational Science and Its Applications - ICCSA, 2006, pp. 298–308.

[10] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Trans. Computers, vol. 62, no. 11, pp. 2266– 2277, 2013.

[11] G. D. Crescenzo and V. Saraswat, "Public key encryption with searchable keywords based on jacobi symbols," in INDOCRYPT, 2007, pp. 282–296.

[12] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, 2001, pp. 360–363.

[13] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Computational Science and Its Applications - ICCSA, 2008, pp. 1249–1259.

[14] H. S. Rhee, J. H. Park,W. Susilo, and D. H. Lee, "Improved searchable public key encryption with designated tester," in ASIACCS, 2009, pp. 376–379.

[15] K. Emura, A. Miyaji, M. S. Rahman, and K. Omote, "Generic constructions of secure-channel free searchable encryption with adaptive security," Security and Communication Networks, vol. 8, no. 8, pp. 1547–1560, 2015.

[16] J. W. Byun, H. S. Rhee, H. Park, and D. H. Lee, "Off-line keyword

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

guessing attacks on recent keyword search schemes over encrypted data," in Secure Data Management, Third VLDBWorkshop, SDM, 2006, pp. 75–83.
[17] W. Yau, S. Heng, and B. Goi, "Off-line keyword guessing attacks on recent public key encryption with keyword search schemes," in ATC, 2008, pp. 100–105.
[18] J. Baek, R. Safavi-Naini, andW. Susilo, "On the integration of public key data encryption and public key encryption with keyword search," in Information Security ISC, 2006, pp. 217–232.
[19] H. S. Rhee, W. Susilo, and H. Kim, "Secure searchable public key encryption scheme against keyword guessing attacks," IEICE Electronic Express, vol. 6, no. 5, pp. 237–243, 2009.
[20] H. S. Rhee, J. H. Park,W. Susilo, and D. H. Lee, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," Journal of Systems and Software, vol. 83, no. 5, pp. 763–771, 2010.
[21] L. Fang,W. Susilo, C. Ge, and J.Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Inf. Sci., vol. 238, pp. 221–241, 2013.
[22] I. R. Jeong, J. O. Kwon, D. Hong, and D. H. Lee, "Constructing PEKS schemes secure against keyword guessing attacks is possible?" Computer Communications, vol. 32, no. 2, pp. 394–396, 2009.
[23] R. Cramer and V. Shoup, "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption," in EUROCRYPT, 2002, pp. 45–64.

Authors profile:

CH.LOKESH KIRAN isa student pursuing M.Tech (CSE) in Eswar College of Engineering, Narasaraopet, Guntur, India..

M SARADA is having 3 years of experience in the field of teaching in various Engineering Colleges. At present he is working as Asst. Prof. in Eswar College of Engineering, Narasaraopet, Guntur, India.