International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Identity-based key encapsulation with semantically secure Searchable Public-Key encryption

JOSE JAMES & NEETHU FRANCIS

PG Scholar Dept. of CSE, K.M.P College of Engineering Odakkali, Kerala, India.

Mail Id: - josekajmes@hotmail.com

Assistant Professor Dept. of CSE, K.M.P College of Engineering Odakkali, Kerala, India. Mail Id: - neethufrancis743@gmail.com

Abstract

Presently security problems over internet increases day by day .Existing system gets search time large with the whole number of ciphertexts. That makes recovery from broad database unreasonable. To improve this problem, this paper propose searchable public key cipher texts with unseen structure for keyword explore as fast as feasible lacking sacrificing semantic security of the encrypted keywords. In SPCHS, every one keyword searchable ciphertext are planned by unseen relative, and with the search trapdoor subsequent to a keyword, the smallest amount in sequence of the relations is relate to a look for algorithm as the supervision to discover all corresponding ciphertext capably. We build a SPCHS idea from scrape in which the ciphertext contain a concealed star like structure. We demonstrate our system to be semantically secure in the Random Oracle (RO) model. The search complexity of the proposed scheme depended upon the actual no of cipher text rather than the no of all ciphertext. Lastly we present a generic SPCHS construction from unidentified identity based encryption and clash free full identity malleable identity based key encapsulation mechanism with anonymity.

Keywords: Searchable Public-Key, Public-key searchable encryption, semantic security, identity-based key encapsulation mechanism, identity based encryption

.

1. Introduction

Public-Key encryption with keyword search(PEKS),are described by Boneh et al. in [1],the benefit of PEKS is that the anybody can know the public key of receiver and it can upload a searchable ciphertexts to the server. The receiver can hand over the searchable keyword to the server. Generally, every sender individually encrypts a file and its extracted keywords and sends the consequential

ciphertexts to a server; when the receiver requests to regain the files containing exact keyword, he delegates a keyword look for trapdoor to the server. After that server finds the encrypted files containing the queried keyword without knowing the original files or the keyword itself, and returns the corresponding encrypted files to the receiver. Finally, the receiver decrypts these encrypted files. Objective is to go and protect data, when data is process and becomes information, so data is to be protected and should not be corrupted.Data manipulation is done by the cloud application level security. i.e. application need to go and protect data, the data manipulation by application. [5] The authors of PEKS also introduced semantic security against choosen keyword attacks (SSCKA) in the sense that the server cannot distinguish the ciphertexts of the keywords of its pick before observe the equivalent keyword search trapdoors. It seems a suitable security concept, particularly if the keywordspace has no high min-entropy. Existing semantically secure PEKS scheme take search time least with the total numberof all ciphertexts. This makes salvage from large-scale databases excessive. Therefore, more efficient search performance is important for basically deploying PEKS schemes. One of important work speed up search over encrypted keywords in public key setting deterministic encryption introduced by the Bellare et al. [2]. An encryption system is the deterministic if encryption algorithm is deterministic. Bellare et al.[2] focus on the enabling search over encrypted keyword to the efficient as search for the unencrypted keyword, such a cipher text containing given keyword can retrieve in the time complexity logarithmic in total number of cipher texts. The reasonable because encrypted keywords from tree like structure according to the binary values stored. Deterministic encryption has two inherent limitations. First, keyword privacy can guaranteed for keywords are a priori hard to guess by the adversary. Second,certain information of the message leaks inevitably via ciphertext of the keywords since encryption is deterministic.Hencedeterministic encryption is applicable in special scenarios.Nowadays many sectors are work with cloud technology, as shown in Fig.1 Finance, Telecom, Utilities, Media andentertainment, Retail and Public sectors such different industries in different sectors are work together on multiple natureof cloud platform. Cloud service provider (CSPs), who provide infrastructure to their customer. Customer don't want to scan their database even by CSPs for advertisement of or any other technical reason. [1]

A. Our Motivation and Basic Ideas

We are concerned to provide that highly well-organized search routine with no sacrificing semantic safety in PEKS.We use unseen star-like arrangement produced by keyword searchable ciphertexts. A keyword space is typically of no high min entropy in many scenarios. Semantic security is important to agreement of keyword privacy in such applications. Thus the linear search complication of existing scheme is the most important difficulty to their acceptance. Regrettably, the linear complication seems to be to be expected because the server has to search and check each ciphertext, due to the information that these ciphertexts are indistinguishable to the server. A earlier look shows that there is at rest space to develop explore presentation in PEKS with no sacrifice semantic safety if one cancategorize the ciphertexts with gracefully planned but unknown associations.

Intuitively, if the keyword searchable ciphertexts have an unknown star-like arrangement. Then search over ciphertexts containing particular keywords may be accelerated. Exclusively, assume all ciphertexts of the similarkeyword form a chain by the connected unknown relations, and also an unknown relation exists from a public top to the first ciphertext of every chain. With a keyword look for trapdoor and the top, the server seeks out the first corresponding ciphertext via the equivalent relation from the top. Then a different relation can be disclosed via the establish ciphertext and guides the for ager to search for out the next corresponding ciphertext. By moving on in this way, all identical ciphertexts can be established. Clearly, the search time depends on the definite quantity of theciphertexts contain the query keyword, relatively than on the total number of all ciphertexts. To assurance suitablesafety, the secreted star-like structure should protect the semantic security of keywords, which indicate that limited relations are disclosing only when the equivalent keyword search trapdoor is recognized. Each sender should be able to produce the keyword -searchable ciphertext with the unseen star-like arrangement by the receiver's public-key; the server have a keyword seek out trapdoor should be able to release partial relations, which is interrelated to all similarciphertexts.

2. Related Work

In the earlier year discover on encrypted data has been widely investigated. Since a cryptographic viewpoint, the obtainable work is dividing into two categories. First is Symmetric searchable encryption and second is Public-keysearchable encryption. The search presentation mainly depends on the total number of the ciphertexts containing the queried keyword. For safety, the system is verified semantically protected based on the

Decisional Bilinear DiffieHellman(DBDH) assumption [3] in the RO model. The resultant SPCHS can produce keyword-searchable ciphertextswith an unseen star-like structure. Furthermore, if both the essential IBKEM and IBE have semantic safety and ambiguitythe resultant SPCHS is semantically safe. As present are identified IBE schemes [4], [5], [6], [7] in both the RO model and the usual model, an SPCHS structure is concentrated to collision-free full-identity malleable IBKEM among ambiguity.In 2013, Abdulla et al. projected quite a few IBKEM scheme to assemble Verifiable Random Functions2 (VRF)[8]. We prove that one of these IBKEM scheme is unsigned and collision-free full identity supple in the RO model. In[9], Frere et al. utilize the "approximation" of multilinker maps [10] to create a standard-model description of Bone hand-Franklin(BF) IBE scheme [11].We change this IBE method into a collision-free full-identity flexible IBKEMmethod with semantic protection and ambiguity in the typical replica. Anonymous identity-based broadcast encryption.A somewhat more complex function is unidentified identity-based broadcast encryption with efficient decryption. Acorresponding application was anticipated correspondingly by Barth et al. [12] and Liberty et al. [13] in the establishedpublic-key location.

Carmela R., Garay J.,[14] describe a method is "Searchable Symmetric Encryption". Symmetric searchableencryption is also described as a Symmetric key encryption with keyword search. This primal was introduced by SongD. X., Wagner D[15].This scheme required linear search time among the range of the database. Goh E-J., Bellovin S.,Agrawal R., Chang Y-C. ,Boldyreva A. they are also follow this follow a line of investigation and filter Song etal.'s original work. The SEKS scheme has been verified to be semantically secure next to an adaptive opponent. It allows the search to be process in logarithmic time, even though the keyword searching require length linear with the size of the database. According to above efforts dedicated to either verifiable security or better search performance .The work in the above system is extended SEKS to the multi-sender state. Wang Q.proposed by "Fuzzykeyword look for over encrypted information in cloud computing". As make unclear Computing become widespread,extra and extra receptive information are creature national into the shade. Even though usual searchable encryption scheme permit a user to securely search greater than encrypted data all the way through keywords and selectively repossess files of interest, these techniques support only accurate keyword search. In this paper, meant for the first time we make official and explain

the problem of helpful fuzzy keyword search larger than encrypted shade data whereas maintaining keyword isolation. Fuzzy keyword investigate seriously enhance collection usability by frequent the identical files whilst users' searching inputs exactly counterpart the predefined keywords or the closest promising similar files based on keyword correspondence semantics, as soon as exact match fails.The Waters .B.R.present the practical applications of SEKS and employs it to understand secure andsearchable audit logs.Chase M. proposed to a encrypt prepared data and a secure method to search that data. In ontop of PEKS schemes, the search complication take time linear with the numeral of all cipher text. during a unconscious production of keyword search trapdoor is to preserve the isolation of the keyword adjacent to a inquiring trapdoor production. Kamara S. proposed to support the dynamic update of the encrypted data and dynamicsearchable symmetric encryption.

Searchable symmetric encryption (SSE) allow a client to encrypt its data in such a technique that this statistics can unmoving be searched. The a large amount instantaneous submission of SSE is to shade storage, someplace it enable aclient to securely farm out its data to an untrusted shade bringer exclusive of sacrifice the ability to search over it. SSE have been the focal point of on the go examine and a huge amount of schemes that accomplish a mixture of levels of safety measures and efficiency have be projected. Any useful SSE arrangement, on the other hand, should satisfy the subsequent property: sublinear search time, protection alongside adaptive preferred keyword attacks, compact guide and the capacity to add and delete files resourcefully.Additional improved extra security in at the cost of the large index. Cash D. planned by Dynamic searchable encryption in extremely huge database. This scheme simultaneously achieve strong security and high efficiency.Dynamic Searchable Symmetric Encryption (DSSE) enable a consumer to achieve keyword query and keep informed operation on the encrypted organizer collections. DSSE has more than a few important applications such as privacy-preserving data outsourcing for computing clouds. In this document, we residential a new DSSE format that achieve the maximum time alone in the middle of all compared alternative with little in sequence escape, noninteractive and professional updates, compressed client storage space, low attendant storage space for huge file keywordpair with an trouble-free intend and accomplishment. Our method achieve these advantageous properties withan extremely effortless figures arrangement (i.e., a bit matrix supported with two static hash tables) that enables resourceful yet secure

explore/inform operation on it. We establish that our method is protected and established that it is realistic with huge number of file-keyword pair smooth with an accomplishment on trouble-free hardware configurations.

The similar work on PEKS, Abdulla et al. [28] file some gaps write reliability for PEKS and deals with the conversion among primitives related to PEKS .some labors have also been dedicated to make PEKS flexible. The work of this type include conjunctive search variety search compartment search , time-scope search , parallel search , allowed search , impartiality test between mixed cipher texts , and fuzzy keyword search . Searchable encryption is worn to prop up search over encrypted data store on shade servers. Established searchable encryption no more than chains accurate keyword searches as a substitute of supplementary bendable fuzzy keyword search.To explain this dilemma, a topical promising arche type, name fuzzy keyword searchable encryption, has been projected. In attendance have been some proposal considered for fuzzy keyword explore in the symmetric key situation,but not a bit efficient scheme in the public key setting. In this paper, we proposition a new primal of interactive publickey encryption with fuzzy keyword search (IPEFKS), which chains proficient fuzzy keyword search greater than encrypted figures in the public key background. We construct and spend a homomorphism encryption base IPEFKSsystem. In adding together, Arriaga et al. projected a PEKS scheme to maintain the isolation of keyword searchtrapdoors.

A chain-like construction is describing to velocity awake the search on encrypted keywords. One can message that the sequence in cannot be completely unseen to the server and drip the reliability of the keywords. To recognizea resourceful keyword search, Bellaire et al. [2] introduce deterministic public key encryption (PKE) and dignified asecurity concept “as strong as possible”. A deterministic searchable encryption system allow capable keyword searchas condition the keywords be not encrypted.Bellare et al. [2] as well obtainable a deterministic PKE system and a general revolution starting a randomized PKE toward a deterministic PKE in the random oracle model. Afterward, deterministic PKE scheme protected in theusual model be in parallel projected next to Bellare et al. and Boldyreva et al.. Particularly we think about seven thinking of isolation for deterministic encryption, together with six forms of semantic protection and an indistinguishability view, and show them all corresponding.We then current a deterministic method for the protected encryption of consistently and independently spread lettersbased exclusively on the subsistence of

trapdoor in one direction permutation. The earlier uses common convolutionassumption and the structure are common, while the final exploit substantial complexity guess and have enhancedefficiency. Brakerski et al. projected the deterministic PKE scheme by way of enhanced security, even thoughthese schemes are at a halt not semantically secure. So far, deterministic PEKS schemes can agreement semanticsecurity simply condition the keyword freedom has a soaring min-entropy. If not, an opposition can extort the encrypted keyword as a result of a straightforward encrypt-and-test bother. Therefore, deterministic PEKS schemes are relevant to application somewhere the keyword space is of a high min-entropy.

3. Implementation

A Problem statement:

From above related work we have addressed following problems in existing system:

- Existing semantically secure public-key searchable encryption schemes take search time linear with the total number of the ciphertexts.
- Makes retrieval from large scale databases prohibitive.
- The local privacy only contains the relationship of the new generated cipher texts.
- Deterministic encryption is only applicable in special scenario.

B] Proposed System as a solution for existing system:

In our proposed system we provide more security as well as we search keyword in a specified file not overalldatabase that make a minimization of time and search keyword as fast as possible without sacrificing semantic security.Build a generic SPCHS construction with Identity-Based Encryption (IBE) and collision-free full-identity malleableIBKEM.

C] Our Work:

We initiate by officially defining the idea of Searchable Public-key Ciphertexts with secret Structures and its semantic security. In this new conception, keyword searchable ciphertexts with their unknown structures can begenerated in the public key location; with a keyword look for trapdoor, incomplete associations can be disclosed toshow the innovation of all corresponding ciphertexts. Semantic security is definite for both the keywords and theunknown structures. It's worth noting that this new perception and its semantic safety are appropriate for keyword searchableciphertexts with any kind of unknown structures. In difference, the idea of conventional PEKS does notinclude any unseen structure between the PEKS ciphertexts; likewise, its semantic safety is only defined for thekeywords.We build a straightforward SPCHS from scrape in the random oracle (RO) model. The system

generateskeyword-searchable ciphertexts with a secret star-like structure. The search presentation mostly depens on the realnumber of the ciphertexts contain the query keyword. For safety, the system is established semantically safe based onthe Decisional Bilinear Diffie- Hellman (DBDH) hypothesis in the RO model. We are also paying attention inprovided that a standard SPCHS building to produce keyword-searchable ciphertexts with a secret star-likeconstruction. Our standard SPCHS is stimulated by several exciting explanation on Identity-Based Key EncapsulationMechanism (IBKEM). In IBKEM, a sender encapsulates a key K to an intentional receiver ID. Of course, receiver IDcan encapsulate and achieve K, and the sender know that receiver ID will achieve K. conversely, a non-intendedreceiver ID0 may also try to encapsulate and achieve K0. We examine that, (1) it is typically the case that K and K0 areself-determining of every other from the view of the receivers, and (2) in some IBKEM the sender may also know K0obtained by receiver ID0. We refer to the former goods as conflict freeness and to the latter as full-identity malleability.An IBKEM scheme is said to be collision-free full-identity impressionable if it possesses both properties. We build ageneric SPCHS construction with Identity-Based Encryption and collision-free full-identity malleable IBKEM.

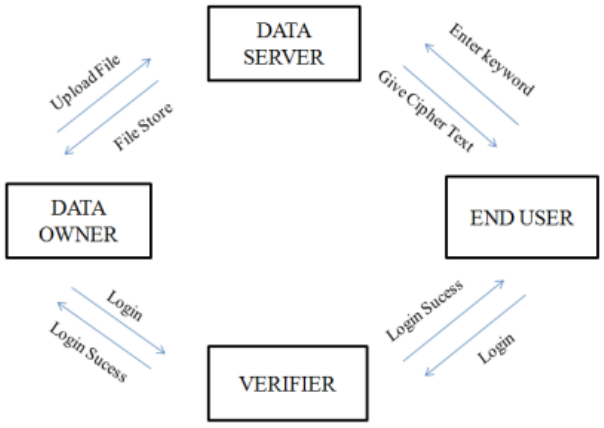

FIGURE 1: BLOCK DIAGRAM

Above diagram contains four models

1] Data Owner.

2] Data Server.

3] End User

4] Verifier.

1] Data Owner: =Data Owner firstly login and then it upload a file into the data server. Then that files are successfullystored by the data server. Ituploads the files with searchable keyword.

2] Data Server: =Data server is stored server files. Dataserver also detects the attacker and attacker's entry will be storedby the data server in the database. All transactions record is also stored by the data server. Dataserver gives the secretkey to the end user. It also gives the file to the end user for download.

3] End User: =End user firstly login after that it will be send the cipher text to the data server. After that data serverpasses a public key. Then end user will be giving the file name to the data server. If the file name

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

present in the data serverwith respected keyword then and then only that file are download otherwise not. It gives file with their ratio and delay.

4] Verifier: =Verifier is to check the entry of the both data owner and end user. If the entry are present in thedatabase then and then only data owner and end user are login successfully otherwise it rejected by the verifier.

4. Experimental Work

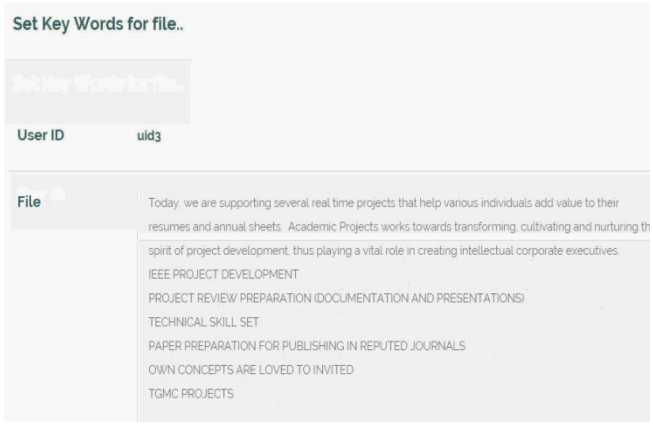

Fig 2: Set Keywords for File.

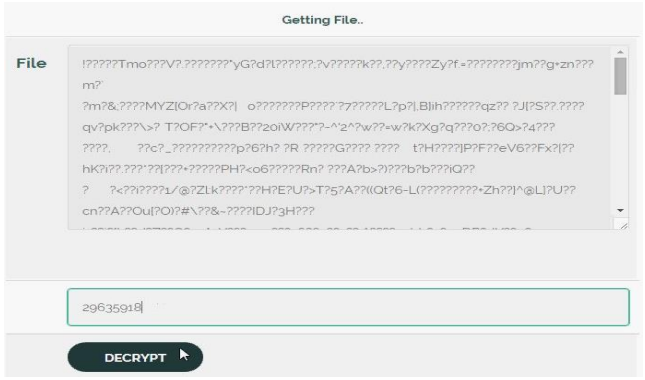

Fig 3: File in Encrypted Format.

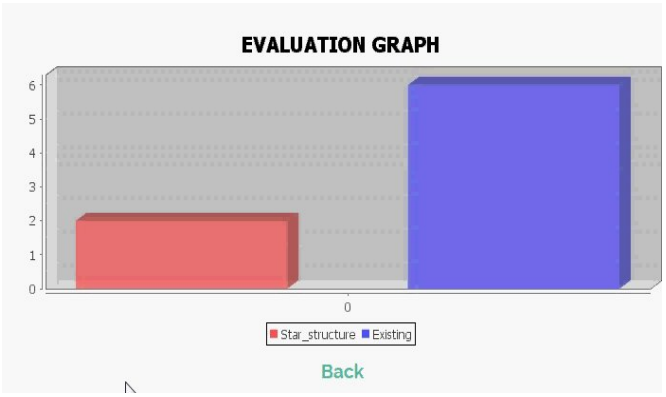

Fig 4: Graph Evolution of System.

5. Conclusion

We investigated fast keyword search in PEKS with semantic security. Proposed the concept of SPCHS as analternate of PEKS. The new concept allows keyword searchable cipher text generated with the hidden structure. Given keyword search trapdoor, search algorithm of SPCHS can disclose part of the hidden structure for guidance on finding out the cipher text of the queried keyword. Semantic security of SPCHS captures privacy of the keyword and invisibility of the hidden structures. The scheme generated keywords searchable cipher texts with the hidden star likestructure.The identified several interesting properties that is collision freeness and full identity malleability in someIBKEM instances and formalized this properties to build a generic SPCHS construction. Applications may be achieveretrieval completeness verification which is the preeminent our comprehension and not been achieved in existing PEKSschemes. Another application may understand public key encryption with

the content search and similarfunctionality realize by the symmetric searchable keyword encryption. Such kind of content searchable encryption isuseful the practice for e.g. Filter the encrypted spasm. The hidden tree like structure between the sequentially encrypted words in the file. Obtain public key searchable encryption allowing content a search.

6. References

[1] Boneh D., Crescenzo G. D., Ostrovsky R., Persiano G.: Public Key Encryption with Keyword Search. In: Cachin C., Camenisch J. (eds.) EUROCRYPT2004. LNCS, vol. 3027, pp. 506-522. Springer, Heidelberg (2004)

[2] Bellare M., Boldyreva A., O'Neill A.: Deterministic and Efficiently Searchable Encryption. In: Menezes A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp.535-552. Springer, Heidelberg (2007)

[3] Boneh D., Boyen X.: Efficient Selective-ID Secure Identity-Based Encryption without Random Oracles. In: Caching C., Camelish J. (eds.) EUROCRYPT2004. LNCS, vol. 3027, pp. 223-238. Springer, Heidelberg (2004)

[4] Boyne X., Waters B. R.: Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In: Work C. (ed.) CRYPTO 2006. LNCS, vol.4117, pp. 290-307. Springer, Heidelberg (2006)

[5] Gentry C.: Practical Identity-Based Encryptionwithout Random Oracles. In: Vaudenay S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004,pp.445-464.Springer, Heidelberg (2006)

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

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

[8] Abdalla M., Catalano D., Fiore D.: Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions. Journal ofCryptology, 27(3), pp. 544-593 (2013)

[9] Freire E.S.V., Hofheinz D., Paterson K.G., Striecks C.: Programmable Hash Functions in the Multilinear Setting. In: Canetti R., Garay J.A. (eds.) Advancesin Cryptology - CRYPTO 2013. LNCS, vol. 8042,pp. 513-530. Springer, Heidelberg (2013)

[10] Garg S., Gentry C., Halevi S.: Candidate Multilinear Maps from Ideal Lattices. In: Johansson T., Nguyen P. (eds.) Advances in CryptologyEUROCRYPT2013. LNCS, vol. 7881, pp. 1-17. Springer,Heidelberg (2013)

[11] Boneh D., Franklin M.: Identity-Based Encryption from the Weil Pairing. In: Kilian J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213-239. Springer,Heidelberg (2001)

[12] Barth A., Boneh D., Waters B.: Privacy in Encrypted Content Distribution Using Private Broadcast Encryption. In: Di Crescenzo G., Rubin A.(eds.) FC2006. LNCS, vol. 4107, pp. 52-64. Springer, Heidelberg (2006)

[13] LIBERT B., PATERSON K. G., QUAGLIA E. A.: ANONYMOUS BROADCAST ENCRYPTION: ADAPTIVE SECURITY AND EFFICIENT CONSTRUCTIONS IN THESTANDARD MODEL. IN: FISCHLIN M., BUCHMANN J., MANULIS M. (EDS.) PKC 2012. LNCS, VOL. 7293, PP. 206-224. SPRINGER, HEIDELBERG(2012)