ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Cloud Technique for Aggregate Key Sharing Mechanism

R. U. Patil, Prof. A. J. Kadam

M. E Student, Department of Computer Engineering, All India Shri Shivaji Memorial Society's , College of Engineering Pune, Savitribai Phule Pune University , Pune India.

Professor, Department of Computer Engineering, All India Shri Shivaji Memorial Society's, College of Engineering Pune, Savitribai Phule Pune University , Pune India.

ABSTRACT: An efficient cryptographic approach for data sharing where datais shared among a group of users as Data sharing is an important functionality in cloud storage. How to securely and efficientlyshare a collection of data related to any subject areas with others in cloud storage. Development of new novel concept of Key- Aggregate Searchable Encryption (KASE). This concept is implemented through development of a concrete key-aggregate searchable encryption framework scheme. This scheme is described as where a data owner only needs to generate and distribute a single aggregate key to a data user for sharing a large number of documents and on the other side user only needs to submit a single aggregate trapdoor to the cloud server, so that he/she can query over the shared documents by the help of generated single aggregate trapdoor. This proposesscheme is perfectly more secure and practically efficient. It is an effective method which is considered as best solution to build a practical data sharing system based on public cloud storage. A detailed review of various methods used for data access controls and encryption is presentedand a brief comparison among the discussed methods is given.Multi cloud scheme reduce storage overhead of thecustomer by compressing the data and reduce computationaloverhead of the cloud storage server.

KEYWORDS: Searchable encryption, data sharing, cloud storage, data privacy

I. INTRODUCTION

Business users are also being attracted towards using the cloud storage due to its advantages. However, while sharing data through cloud storage, users have to simultaneously aware about the data leakages in the cloud. Many times business organizations need to share the confidential data within the organization or to the other organizations. Consider a scenario where a manager wants to share multiple confidential files with one of the employee then manager will upload suppose n number of files on cloud storage and will provide n number of encryption keys to the employee. The employee will store all the keys securely. Then using these keys, the employee will generate the keyword trapdoor for accessing the files. So for n number of files, it is not efficient to provide n number of keys, store them securely and then generate trapdoors for each file. It becomes very expensive at the employee's side server. This practical problem motivates to construct a scheme which will provide a single aggregated key to the employee and will allow access to the cloud by generating single trapdoor by the employee to access any number of files.In this paper, I propose the novel concept of key-aggregate searchable encryption (KASE), and instantiating the concept through a concrete KASE method. The propose KASE scheme relates to any cloud storage that supports the searchable group data sharing feature, which means any user may prefer to distribute a group of files which are selective with a group of selected users, while permitting the final to carry out keyword search above the earlier. To maintain searchable group data sharing the main needs for efficient key management are double. Primarily, a data owner wants to allocate a single aggregate key (instead of a group of keys) to a user for sharing any number of files. Subsequent, the user needs to submit a single aggregate trapdoor to the multi cloud for performing keyword search over any quantity of shared files. KASE scheme can assure both requests.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

II. LITERATURE SURVEY

Monica G. Charate1, Dr. Savita R. Bhosale proposed a Cloud Computing Security Using Shamirs Secret Sharing Algorithm From Single Cloud to Multi Cloud. This paper is carried out to design single and multi-cloud using secret key sharing algorithm which will result in deduction of the cost for the physical infrastructure, reducing the cost entry and execution as well as the response time for various associated applications. In this paper ,I have referred the solution for performance of the Shamirs secret sharing scheme, is used in a multi cloud environment [1]. AdlaShekhar, JanapatiVenkata Krishna proposed a Secure and Reliable Cloud Security from Single to Multi Clouds. This paper studies recent investigation related to single and multi-cloud security and addresses. It is found that the investigation into the use of multi-cloud service providers to keep security has received less attention from the study community than has the use of single clouds. This effort aims to help the use of multi clouds due to its capability to reduce security threats that move the cloud computing user [2]Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee, and Wenjing Lou, design a Secure Deduplication with Efficient and Reliable Convergent Key Management. In this paper, I have referred Proof of ownership, Convergent encryption, Key management, Security of Convergent Encryption Key [3]. Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and RobertH. Deng, proposed a Key-Aggregate Cryptosystem forScalable Data Sharing in Cloud Storage. In this paper, Ihave referred Cloud storage, Data sharing, Key-aggregateencryption, Patient-controlled encryption, Compact Keyin Symmetric-Key Encryption, Compact Key in Identity-Based Encryption [4]. X. Liu, Y. Zhang, B. Wang, and J. Yan, proposed Mona: Secure multi-owner data sharing for dynamic groups in the cloud and from this paper I have referred secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud [5].Ms.V.Mangaiyarkkarasiand Mr.K.A.Dhamodaran proposed A Comparative Surveyon Availability and Integrity Verification in Multi-Cloud. This survey paper provides overview about variousProvable Data Possession techniques in cloud. In thisPaper, I have referred the solution of various availabilityand integrity verification schemes and its methodologyare classified along with their adaptation to single/multicloud environment [6]. R. Lu, X. Lin, X. Liang, and X. Shen, proposed Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing. In this paper, I have referred information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents [7]. CongWang, Qian Wang, and KuiRen Privacy-Preserving PublicAuditing for Data Storage Security in Cloud ComputingProposed Privacy-Preserving Public Auditing for DataStorage Security in Cloud Computing. In this paper,utilization and uniquely combine the public key basedhomomorphic authenticator with random masking toachieve the privacy-preserving public cloud data auditingsystem, which meets all requirements. To support efficienthandling of multiple auditing tasks,further explore thetechnique of bilinear aggregate signature to extend mainresult into a multi-user setting[8]. Y. Hwang and P. Lee, proposed a Public key encryption with conjunctive keyword search and its extension to a multi-user system. In this paper I have referred the PECK scheme provides the document search containing each of several keywords over a public key setting [9]. Dawn Xiaodong Song, David Wagner, Adrian Perrig, proposed a Practical Techniques for Searches on Encrypted Data. In this paper, I have referred Searching on Encrypted Data, Sequential Scan, Controlled Searching, Support for Hidden Searches [10].

III. EXISTING SYSTEM APPROACH

There is a rich literature on searchable encryption, including SSE schemes and PEKS schemes. In contrast to those existing work, in the context of cloud storage, keyword search under thematic-tenancy setting is a more common scenario. In such a scenario, the data owner would like to share a document with a group of authorized users, and each user who has the access right can provide a trapdoor to perform the keyword search over the shared document, namely, the “multi-user searchable encryption” (MUSE) scenario. Some recent work focus to such a MUSE scenario, although they all adopt single-key combined with access control to achieve the goal. In, MUSE schemes are constructed by sharing the document’s searchable encryption key with all users who can access it, and broadcast encryption is used to achieve coarse-grained access control. attribute based encryption (ABE) is applied to achieve fine-grained access control aware keyword search. As a result, in MUSE, the main problem is how to control which users can access which documents, whereas how to reduce the number of shared keys and trapdoors is not considered. Key aggregate searchable encryption can provide the solution for the latter, and it can make MUSE more efficient and practical.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

IV. PROPOSE SYSTEM APPROACH

In this paper, we address this challenge by proposing the novel concept of key-aggregate searchable encryption (KASE), and instantiating the concept through a concrete KASE scheme. The propose KASE scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users, while allowing the latter to perform keyword search over the former. To support searchable group data sharing the main requirements for efficient key management are twofold. First, a data owner only needs to distribute a single aggregate key (instead of a group of keys) to a user for sharing any number of files. Second, the user only needs to submit a single aggregate trapdoor (instead of a group of trapdoors) to the cloud for performing keyword search over any number of shared files. To the best of my knowledge, the KASE scheme proposed in this paper is the first known scheme that can satisfy both requirements (the key-aggregate cryptosystem , which has inspired this work, can satisfy the first requirement but not the second).

I first define a general framework of key aggregate searchable encryption (KASE) composed of seven polynomial algorithms for security parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing. I then describe both functional and security requirements for designing a valid KASE scheme.
I then instantiate the KASE framework by designing a concrete KASE scheme. After providing detailed constructions for the seven algorithms, I analyze the efficiency of the scheme, and establish its security through detailed analysis.
I discuss various practical issues in building an actual group data sharing system based on the propose KASE scheme, and evaluate its performance. The evaluation confirms this system can meet the performance requirements of practical applications.

V. SYSTEM ARCHITECTURE

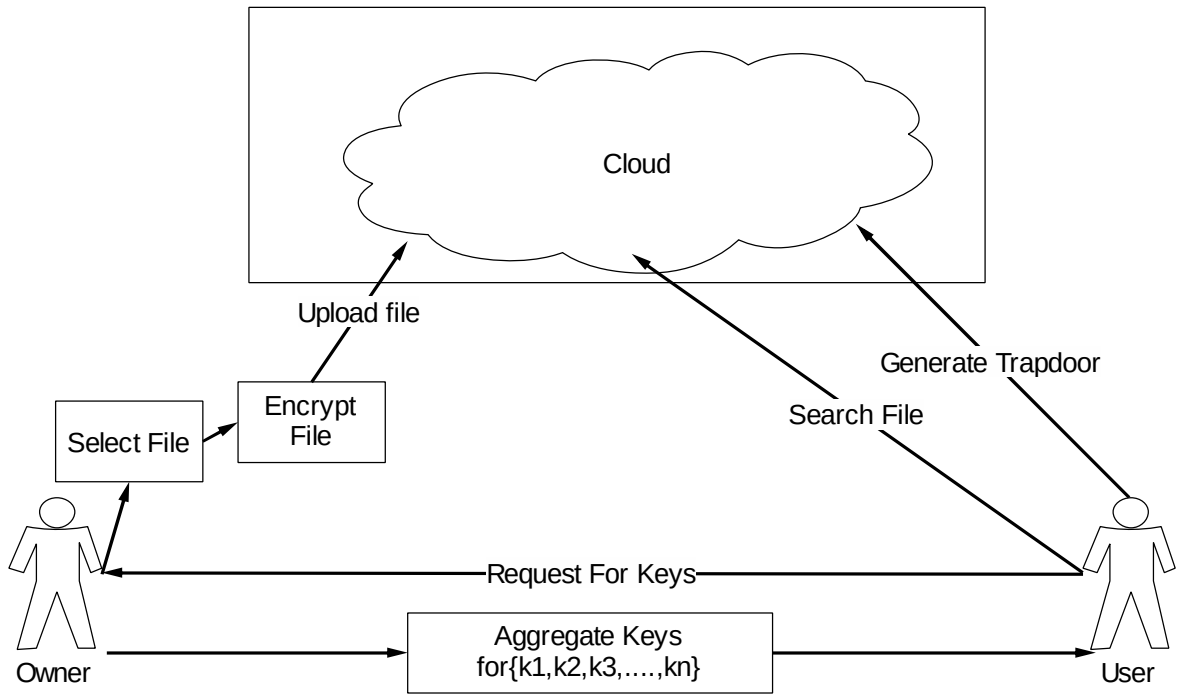


Fig.1. Propose System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

MODULE DESCRIPTION

1. KEY GENERATION
In this module admin going to generate two keys for encryption and decryption process.By using Asymmetric algorithm, admin going to generate master secret key and public key.

2. ACCESS CONTROL
In this module admin going to give access control for the files he will going to upload, while uploading admin going to encrypt the file with the help of master secret key for the security purpose to the cloud.

3. KEYWORD INDEXING
Remove un-necessary words from the file and Find the keywords. Calculate the Content Weight age of keywords Convert the Keywords into hash code by using MD5 algorithm; place the hash code in Index Array.

4. SEND AGGREGATE KEY
Based on the categories selected by admin, system has to fetch the corresponding hash keys + fetch the Public Key. Generate the User Aggregate Key and finally send it to users.

5. SEARCH WITH KEYWORD
User has to select the aggregate Key then after that Input the search keyword. Convert the keyword into hash code .Decrypt the aggregate Key, Separate and get hash keys and separate and get public Key. Using Hash Key and keyword generate hash codes (Trapdoor). Send the Hash codes to server, based on the Hash codes received server has to check the keyword index and if any matching files are available, list all the file names to the user. (Adjust & Test)View the shortlisted files from server, download the files and finally decrypt the file with owner public key**.**

VI. MATHEMATICAL MODEL

Input
Input given to the system is: - File in any format.

Output
I check or test the result of the keys aggregation, trapdoor generation, file stored into cloud.

Process

Step 1: Data owner Select File
Step 2: Encrypt File (For encryption we user AES or RSA).
Step 3: Upload file on cloud
Step 4: User search file on cloud
Step 5: Send key request to Data owner
Step 6: Data owner receive key request and Aggregate the keys
Step 7: Send keys to user
Step 8: User receives keys and generate trapdoor
Step 9: File decryption
Step 10: Download file

VII. EXPERIMENTAL RESULT

Considering that the algorithms including KASE. Setup, KASE. Adjust and KASE. Test are only run in the cloud server, only the execution times in computer are tested. As shown in Fig. 2, I can see that: 1) The execution time of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

KASE. Setup is linear in the maximum number of documents belonging to one owner, and when the maximum number grows up to 20,000, it is reasonable that KASE. Setup algorithm only needs 259 second. 2) The execution time of KASE. Encrypt is linear in the number of keywords, and when the number grows up to 10,000, KASE. Encrypt algorithm only needs 206 second in computers, but 10,018 second in mobile devices. Therefore, I can draw two conclusions; one is that it is not feasible to upload document with lots of keywords using a mobile phone;

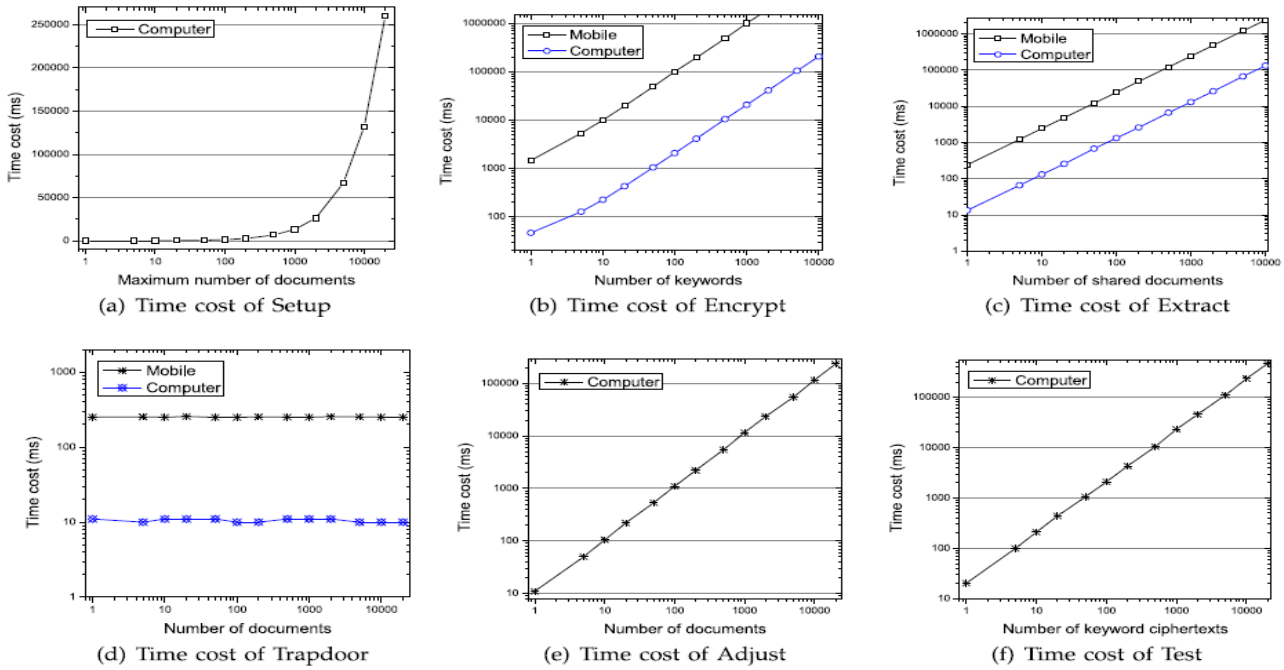


Fig. 2. Time cost of KASE algorithms.

the other is that the keyword search with pairing computation can be executed quickly in computers now. 3) The execution time of KASE. Extract is linear in the number of shared documents, and when the number grows up to 10,000, KASE. Extract algorithm only needs 132 second in computer, but 2,430 second in mobile devices. Because the KASE. Extract always runs along with the KASE. Encrypt, it is not suggested to be executed in the mobile devices. 4) The execution time of KASE. Trapdoor is a constant, i.e., 0.01 second in computer and 0.25 second in mobile devices. In fact, the mathematical operation in KASE. Trapdoor is the once multiplication in G, so that the keyword search can be performed efficiently in both mobile devices and computer. Compared with other schemes, there is a significant improvement in this scheme. 5) The execution time of KASE. Adjust is linear in the number of documents. In fact, it can be improved in the practical application. 6) The execution time of KASE. Test is linear in the number of keyword cipher texts. In fact, the mathematical operation in KASE. Test is twice as much as the pairing computations. When the number grows up to 20,000, it will take 467 second.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

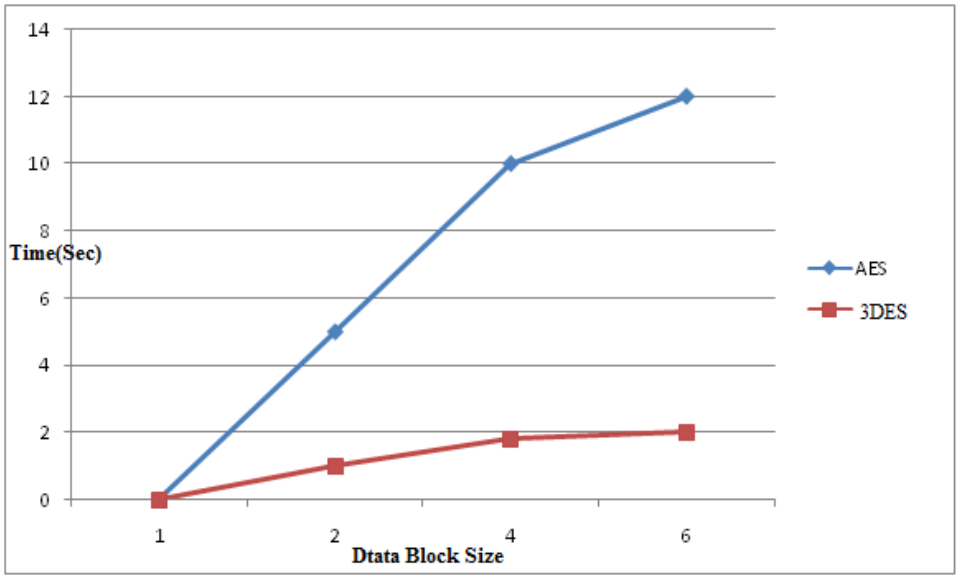
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

VIII. PERFORMANCE MEASURES AND EFFICIENCY CALCULATION

Performance with ECB



Encryption Performance comparison with ECB
Result Table

Data Block Size	AES	3DES
1	0	0
2	5	1
4	10	1.8
6	12	2

Description

ECB(Electronic Codebook Mode) is the basic form of clock cipher where data blocks are encrypted directly to generate its correspondent ciphered blocks.Compared to all other algorithms the AES algorithm has made its mark in the cryptographic field. The unbeatable strength of the encryption algorithm is mainly depended upon the key length. The results show the impact of changing data load on each algorithm and the impact of Cipher Mode used.The results show the superiority of AES algorithm over other algorithms in terms of the processing time. It shows also that 3DES consumes more resources when the data block size is relatively big.

IX. CONCLUSION

Considering the practical problem of privacypreservingdata sharing system based on public cloudstorage which requires a data owner to distribute alarge number of keys to users to enable them to accesshis/her documents, we for the first time proposethe concept of key-aggregate searchable encryption(KASE) and construct a concrete KASE scheme. Both analysis and evaluation results confirm that my workcan provide an effective solution to building practicaldata sharing system based on public cloud storage.In a KASE scheme, the owner only needs to distributea single key to a user when sharing lots ofdocuments with the user, and the user only needsto submit a single trapdoor when he queries overall documents shared by the same owner. Multi cloud schemereduce storage overhead of the customer by compressing thedata and reduce computational overhead of the cloud storageserver.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

REFERENCES

[1] Monica G. Charate1, Dr. Savita R. Bhosale," Cloud Computing Security Using Shamir's Secret Sharing Algorithm From Single Cloud To Multi Cloud", Volume No 03, Special Issue No. 01, April 2015.
[2] AdlaShekhar, JanapatiVenkata Krishna," Secure and Reliable Cloud Security from Single to Multi Clouds", volume 16 number 2 – Oct 2014.
[3]J.Li, X.F. Chen, M.Q. Li, J.W. Li, P. Lee, Wenjing Lou. "Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Transactions on Parallel and Distributed Systems, 25(6): 1615-1625, 2014.
[4] C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.
[5] X. Liu, Y. Zhang, B. Wang, and J. Yan."Mona: secure multi owner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.
[6] Ms.V.Mangaiyarkkarasiand Mr.K.A.Dhamodaran," A Comparative Survey on Availability and Integrity Verification in Multi-Cloud", Volume 1, Issue 10, December 2012.
[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance:The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.
[8] Cong Wang, Qian Wang, and KuiRen"Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing"IEEE INFOCOM 2010.
[9] Y. Hwang, P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In:Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.
[10] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.