AN ALGORITHM TO SECURE DATA FOR CLOUD STORAGE

Roshan Jahan[1], Preetam Suman[2], Deepak Kumar Singh[3]
[1]Assistant Professor, Integral University, Lucknow (India),
roshan@iul.ac.in
[2]Assistant Professor,Jaipuria Institute of Management, Lucknow
preetam.suman@jaipuria.ac.in,
[3]Associate Professor,Jaipuria Institute of Management, Lucknow
d.singh@jaipuria.ac.in,.

Abstract: Now a day's cloud computing is the backbone of the digital world. Cloud service providers every type of service needed by consumers. It offers various resources to all consumers by dynamic allocation for guaranteed services. One of the major services of storage is primarily used by consumers. Many free services for cloud storage are available to use. On the other side, a group of malicious activities increases with an increase in facilities. The malicious activities may change the format of data, which can't be used by users. Some ransomware is very active, which is asking ransoms to recover the data. In view of many examples of security threats, this paper proposes a mechanism for data security. This paper describes a security algorithm, which is the encryption mechanism of data. The encryption algorithm encrypts all the data stored by cloud users. The algorithm is tested with different sizes and different types of files. It is designed in a manner so that it can work fast and efficiently in the cloud environment.

Keywords: **cloud security, encryption algorithm, data security, cloud computing.**

1. Introduction

Cloud computing [1] is a type of platform in which users can share the resources. It is a type of processing in which users can utilize resources accessible on cloud framework. In other words, it can be described as the place where resources can be accessible through the system. Cloud computing permits the client to utilize innovation empowered administrations through the web. Distributed cloud is web-based assistance where the client can undoubtedly utilize capacity, administrations without knowing how it is really functioning inside. Distributed computing is an assortment of virtual machines where the client just uses the administrations gave by the virtual machines they don't have a control on virtual machines. In distributed computing, a few associations store their information on a solitary virtual server once in a while numerous working frameworks are executed on a solitary virtual server; for this situation, there are odds of danger from other machines. So there is a need for elevated level security, particularly out in the open cloud framework.

There are many advantages of cloud computing which are offered to users. The most important advantage of cloud technology is the physical location of a resource is open to the client. The client just needs to connect with a device. Cloud computing also helps in disaster management. Likewise, a solitary asset or gadget can be shared among numerous clients—these aides in accomplishing better use. A cloud administration is considered as increasingly solid as the cloud specialist organization looks after reinforcements. Cloud innovation additionally boosts adaptability and flexibility as cloud administrations utilize a pool of resources. Midway oversaw information, and the protection among projects and information makes it increasingly secure. A cloud framework can provide similar interface to all the users by utilizing smart software.

Cloud computing innovation additionally carries numerous difficulties alongside amazing advantages [2]. There are many problems associated with the cloud computing. One of the problem which is mostly noted by researchers is cloud security. Other than security of cloud, interoperability, vender lock-in and compliance are other significant concerns that come into the picture. Visit occasions of security and protection breaks, make them head the rundown. Be that as it may, the danger of consistency and interoperability is diminishing gradually and bites by bit. Lock-in still frequents clients from giving over their valuable information to the mists. Aside from these, SLA level, computational, and information level difficulties are additionally there.

A report prepared by Crowd Research Partners states that cloud security is a major concern for cloud clients and security experts. However, a Right Scale report expresses that "As organizations become progressively experienced with cloud, the top challenges shifts. Security is the biggest issue among cloud learners, while cost turns into a greater test for moderate and propelled clients.".

As data is picking up significance in this computerized time, it is drawing in light of a legitimate concern for data frauds and programmers and, in this way, turns into a prime concern for

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

security experts [3]. In cloud innovation, physical storage resources are shared among clients, which draws in the danger of unapproved access to information. The client consistently remains in anxiety about data loss and information leak.

This paper proposes an encryption algorithm to secure the data stored on cloud storage. The algorithm encrypts the data so that it can’t be readable. The algorithm proposed in this paper is very difficult to break. The data encoded by algorithm is very difficult to be retrieve without the key. It fulfils all the needs and requirements of cloud computing.

2. Literature Survey

D. Zhe et. Al. [4] depicted the information security issue and malicious attacks in his paper. cloud storage security concerns the client's information security. The author of the paper depicted the security strategy identified with information security of cloud storage.

A. Sun et al. [5] have given a quantifiable security assessment framework for various cloud platform. It consists of a security checking, recuperation, assessment model, and a visual module. Author described the security mechanisms to secure cloud storage.

J. Shen et al. [6] introduced a square plan based key understanding convention, which can deftly expand the quantity of members in a cloud domain as indicated by the structure of the square plan. In light of the proposed bunch information sharing model, the creator has introduced general recipes for producing the basic meeting key IC for various members.

V. P. Lalitha et al. [7] has actualized a calculation that can store the information in the server in an encoded manner, and just the administrator has the consent to decode the information. The calculation can likewise recognize unapproved access and furthermore can hinder the specific IP address.

L. Qing et al. [8] has depicted the different security issues identified with the private cloud for undertakings. The creator has examined security issues in all the potential angles.

M. Nanda et al. [9] has talked about different security dangers in distributed computing. The creator directed a writing review to decide the consciousness of these attacks among the different Cloud Computing clients.

Y. Reddy [10] has talked about the problems associated with the data on cloud storage. Author described the security model for the security of cloud.

R. A. R. Shaikh et al. [11] have proposed an information security estimation device that was utilized to gauge distributed computing information security. The creator has dissected the boundaries for estimating the information security are distinguished, and different cloud administrations to gauge the security.

P. Sha et al. [12] has presented an encryption framework based on the RSA algorithm. The encryption algorithm presented by author also consists of a public key and a private key. These keys were created during the encryption process. It contains a prime number, which was used in Pascal's triangle hypothesis and RSA algorithm model.

X. Tune et al. [13] have presented a half and half distributed computing plan based on the Paillier algorithm. As indicated by the results, the algorithm is promising.

Salma et al. [14] have proposed a half and half structure of Dynamic AES and Blowfish algorithm. The combination of algorithm provide secure transmission of data to cloud storage.

N. Veeraragavan et al. [15] has proposed an algorithm to secure cloud storage. This was an uneven encryption algorithm. The algorithm uses same key for encoding and decoding the data.

D. Pei et al. [16] has proposed a strategy utilizing the Hadoop bunch and uses the MapReduce structure to plan the encryption administration framework. The creator has additionally given a total encryption plot, a particular encryption conspires, and an incomplete encryption plan to encode the video information. Therefore, it improves the speed of video encryption as well as streamlines the video encryption system. Besides, the client can choose the encryption plot as indicated by their necessities. The test results show that the video encryption administration that we give can meet the prerequisites of rapid, security, etc.

S. Mudepalli et al. [17] has proposed a proficient cipher text recovery methods on an enormous volume of data. Author used Blowfish algorithm to encrypt the data. Public key based elliptic bend cryptography (ECC) was used for key generation.

F. S. Wu [18] has proposed the elliptic bend encryption algorithm. It is a streamlined technique which is dependent on the elliptic bend encryption algorithm. Results show the promising outcomes to ensure the security and soundness of cloud storage.

A. S. Awad et al. [19] have introduced another security component utilizing a half and half technique for encryption algorithm and a dissemination framework to upgrade cloud database privacy. The outputs demonstrated that the proposed encryption and half and half discontinuity model gives a protected instrument that improves information secrecy regarding quicker response and extra security.

The above literature review presented research done by various researchers. It can be observed that the requirement of security is very necessary and many algorithms were developed for security of cloud. According to the literatures there is need of more strong encryption algorithm which can be applicable in cloud computing. The algorithm should work with quick response. Following sections will describe the implementation of proposed encryption algorithms.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

3. Proposed Algorithm

Previous section discussed the need of a new algorithm to make data more secure on cloud. This section describes the steps of proposed algorithm.

The algorithm is designed to be operated on 1024-bit plaintext and cipher text. The algorithm is controlled by 1024-bit key to make data more secured. The decryption process is identical to encryption process.

The first step of algorithm is key generation. The algorithm will generate a random key of 1024 bit. After that it will be divided in the blocks of 128 bit. These 8 blocks will be used in initiating to generate another keys. The next keys were generated is a sequence similar to Random kay AES (RK-AES) [20].

Encryption:

Step 1: In the first step a plaintext of 1024 bit is taken.

Step 2: In second step the plaintext of 1024 bit is divided into eight sub-blocks of 128 bits.

Step 3: In third step each sub-block of 128 bit will be added to a key block, generated by Random kay AES (RK-AES) process.

Step 4: In the fourth step each bit will be replaced by another bit using a replacement table.

Step 5: Output of the fourth step will be arranged in 2D matrices.

Step 6: In the sixth step a mirror image will be taken for the matrices arranged in fifth step.

Step 7: Each bit will be shifted to right N times. This N can be calculated as

N= (no. of step) mod (size of block)

Step 8: In the eights step a step-key will be generated using formula initial key/ previous step-key.

Step 9: The step-key will be added in output of previous step.

Step 10: The tenth step will be iteration. There should be 10 iterations to get cipher text.

Implementation of proposed algorithm:

A setup is developed on cloud for the implementation of proposed algorithm. The algorithm requires to be test on real cloud environment, so that it can be used by cloud users. The cloud environment was setup on following configuration.

SSD: 160 GB

RAM: 8GB

Processor: 4vCPU (Intel Xeon Processor)

This configuration is provided as a droplet by Digital Ocean [21].

After setup the environment, the proposed algorithm was implemented using angular js, mysql and java. Mysql database is used to store the file, and keys in encrypted form. Other than proposed algorithm RSA, AES, and Blowfish is also implemented on same infrastructure. So that comparison can be observed.

4. Result and Discussion

The algorithms are evaluated on 6 types of file format. Each file format is having different file size so that each algorithm can be evaluated on different parameters. The files and their details are shown in table 1.

S. No.	File Type	File Size
1.	Text file	0.05 MB
2.	JPG image file	0.1 MB
3.	MS Word file	2 MB
4.	PDF Document	5 MB
5.	MP3 file	10 MB
6.	MP4 file	15 MB

Table 1: File format and file size

The algorithm was evaluated in 5 parameters. The five parameters are encryption time, decryption time, size of file after decryption, avalanche effect, and entropy. The file size taken for evaluation of algorithm is 0.05 MB, 0.1 MB, 2 MB, 5 MB, 10 MB and 15 MB. The flowing graphs shows comparison between the proposed encryption (prop. encry.) algorithm. RSA, AES, and blowfish algorithms are the tested algorithms for encryption, so that these algorithms were chosen for the comparison.

Figure 1 shows the time taken by algorithm to encrypt the file of different sizes. It can be observed that the proposed algorithm takes less time than other algorithms RSA, AES and Blowfish. It can also be observed that encryption time is increasing with the increment in file size.

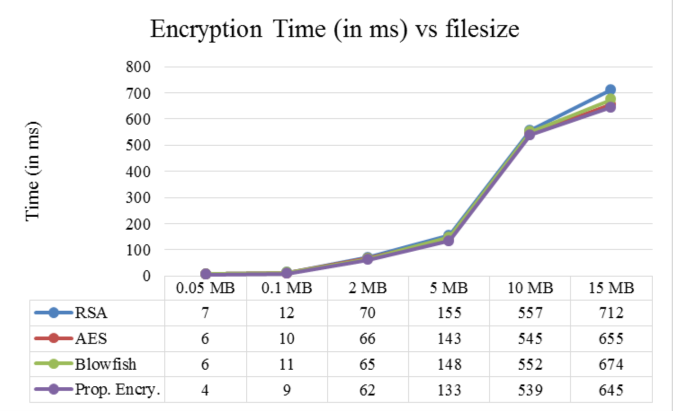
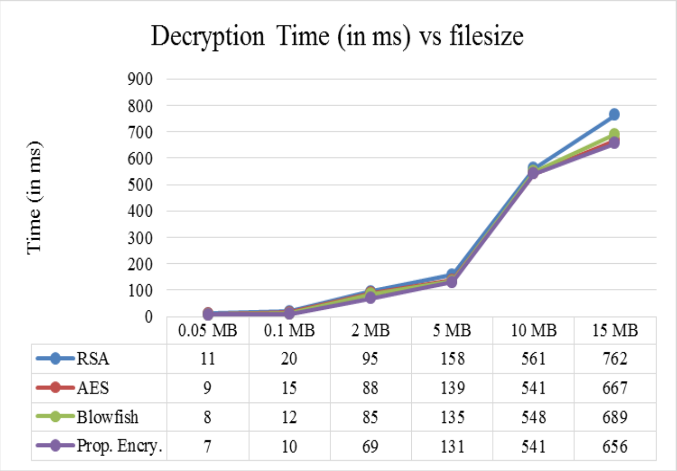


Figure 1: Comparison of encryption time for different file size

Figure 2 shows the time taken by algorithm to decrypt the file of different sizes. The same file has been taken for decryption which were encrypted using algorithm. It can be observed that the proposed encryption algorithm takes less time to decrypt the files than other algorithms RSA, AES and Blowfish. It can also be observed that decryption time is increasing with the increment in file size.

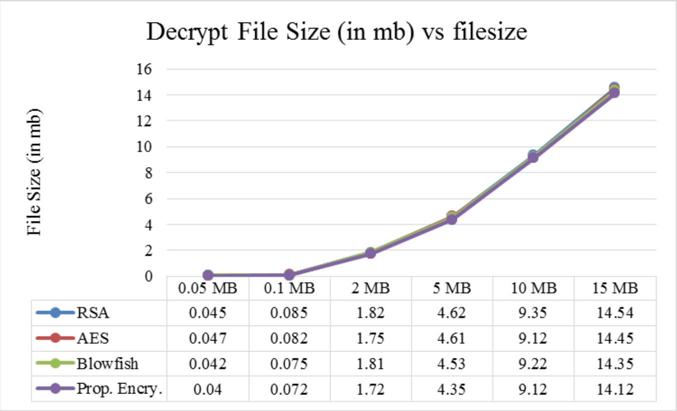
ISSN (Print): 2204-0595
ISSN (Online): 2203-1731



	0.05 MB	0.1 MB	2 MB	5 MB	10 MB	15 MB
RSA	11	20	95	158	561	762
AES	9	15	88	139	541	667
Blowfish	8	12	85	135	548	689
Prop. Encry.	7	10	69	131	541	656

Figure 2: Comparison of decryption time for different file size

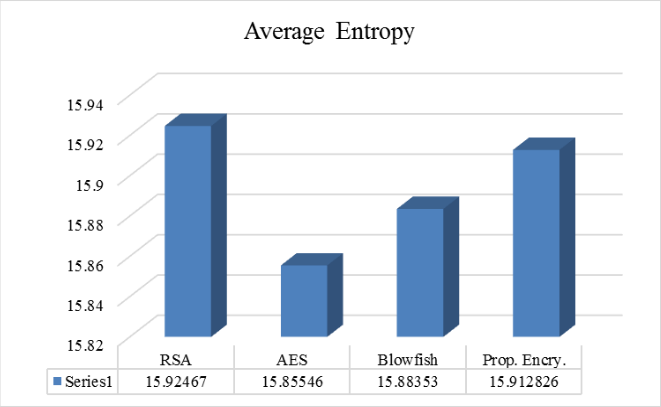
Figure 3 shows the file size after encryption of file of different sizes. The same file has been chosen to observe the comparison. It can be observed that the all the algorithms create very similar size of decrypted files. However, the proposed algorithm creates file of less size than other algorithms RSA, AES and Blowfish. The less size can be useful in the case of storage of more files. Less storage on cloud can contain more decrypted files.



	0.05 MB	0.1 MB	2 MB	5 MB	10 MB	15 MB
RSA	0.045	0.085	1.82	4.62	9.35	14.54
AES	0.047	0.082	1.75	4.61	9.12	14.45
Blowfish	0.042	0.075	1.81	4.53	9.22	14.35
Prop. Encry.	0.04	0.072	1.72	4.35	9.12	14.12

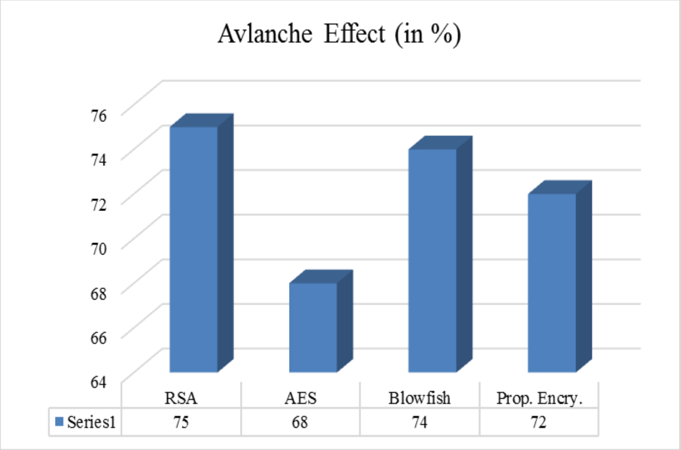
Figure 3: Comparison of decrypt file size for different file size

Figure 4 shows calculation of entropy for algorithm. Entropy is the degree of randomness in the data. Each significant information gives some connection among the data. The entropy should be high for efficient encryption algorithms. The entropy of proposed encryption algorithm is somehow similar to RSA and better then AES and Blowfish algorithm.



	RSA	AES	Blowfish	Prop. Encry.
■ Series1	15.92467	15.85546	15.88353	15.912826

Figure 4: Comparison of average entropy for algorithms



	RSA	AES	Blowfish	Prop. Encry.
■ Series1	75	68	74	72

Figure 5: Comparison of avalanche effect for algorithms

Figure 5 shows avalanche effect for algorithms. Avalanche effect impact expresses that a little change in the data will prompt an extremely enormous change in the output. In figure 5 avalanche effect of proposed encryption algorithm is somehow similar to AES and better then Blowfish. The avalanche effect of RSA is better than other algorithms.

5. Conclusion

Protection and security of data stored on cloud storage is very important for the users. As cloud computing is new for many user so sometimes user can't understand how to protect data. This paper provides an overview of existing security algorithm and techniques. This paper has proposed an encryption algorithm to encode the uploaded documents on cloud storage. The conversation shows that proposed encryption algorithm gives a stronger encryption. It is also observed in the results that the proposed algorithm takes less time for encryption and decryption of files with respect to RSA, AES and Blowfish. Avalache impact and entropy values demonstrates the nature of cipher text created by the proposed calculation is equivalent to industry standards. As depicted in past segments, key quality of proposed encryption algorithm is for all intents and purposes it is difficult to be broken in the near future. Further, the pattern of encryption time shows the proposed algorithm

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

will turns out to be progressively valuable as the file size increases. In any case, equal execution of code piece brings about capacity and registering overhead, which is an exceptionally little cost for better execution. However, studies can be performed for key development, key expansion, key management, cryptanalysis and impact of different attacks in future.

References

[1] Thomas Erl, Ricardo Puttini, Zaigham Mahmood "Cloud Computing: Concepts, Technology & Architecture" Prentice Hall, 2013

[2] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, A Comprehensive Survey on Security in Cloud Computing, Procedia Computer Science, Volume 110, Pages 465-472, 2017.

[3] Shah, Krutika & Vadiya, Vahida & Jhaveri, Rutvij. A Survey Paper on Security in Cloud Computing: A Bibliographic Analysis. Circulation in Computer Science. vol. 1, pages-19-23, 2016.

[4] D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," *2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids)*, Beijing, 2017, pp. 145-149.

[5] A. Sun, G. Gao, T. Ji and X. Tu, "One Quantifiable Security Evaluation Model for Cloud Computing Platform," *2018 Sixth International Conference on Advanced Cloud and Big Data (CBD)*, Lanzhou, 2018, pp. 197-201.

[6] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 996-1010, 1 Nov.-Dec. 2019.

[7] V. P. Lalitha, M. Y. Sagar, S. Sharanappa, S. Hanji and R. Swarup, "Data security in cloud," *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, 2017, pp. 3604-3608.

[8] L. Qing, Z. Boyu, W. Jinhua and L. Qinqian, "Research on key technology of network security situation awareness of private cloud in enterprises," *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, Chengdu, 2018, pp. 462-466.

[9] M. Nanda, A. Tyagi, K. Saxena and N. Chauhan, "Hindrances in the security of Cloud Computing," *2016 6th International Conference - Cloud System and Big Data Engineering (Confluence)*, Noida, 2016, pp. 193-198.

[10] Y. Reddy, "Big Data Security in Cloud Environment," *2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, Omaha, NE, 2018, pp. 100-106.

[11] R. A. R. Shaikh and M. M. Modak, "Measuring Data Security for a Cloud Computing Service," *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, Pune, 2017, pp. 1-5.

[12] P. Sha and Z. Zhu, "The modification of RSA algorithm to adapt fully homomorphic encryption algorithm in cloud computing," *2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS)*, Beijing, 2016, pp. 388-392.

[13] X. Song and Y. Wang, "Homomorphic cloud computing scheme based on hybrid homomorphic encryption," *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, 2017, pp. 2450-2453.

[14] Salma, R. F. Olanrewaju, K. Abdullah, Rusmala and H. Darwis, "Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms," *2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT)*, Makassar, Indonesia, 2018, pp. 18-23.

[15] N. Veeraragavan, L. Arockiam and S. S. Manikandasaran, "Enhanced encryption algorithm (EEA) for protecting users' credentials in public cloud," *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, Chennai, 2017, pp. 1-6.

[16] D. Pei, X. Guo and J. Zhang, "A video encryption service based on cloud computing," *2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Macau, 2017, pp. 167-171.

[17] S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," *2017 International Conference on*

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 267-271.

[18] F. S. Wu, "Research of Cloud Platform Data Encryption Technology Based on ECC Algorithm," *2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, Changsha, 2018, pp. 125-129.

[19] A. S. Awad, A. Yousif and G. Kadoda, "Enhanced Model for Cloud Data Security based on Searchable Encryption and Hybrid Fragmentation," *2019 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, Khartoum, Sudan, 2019, pp. 1-4.

[20] Saha Rahul, Geetha G., Kumar Gulshan, Kim Tai-hoon "RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys", Security and Communication Networks, Hindawi, 2018.

[21] Digital Ocean. Available: https://www.digitalocean.com/ [Accessed: 11-May-2020].

[22] Server Test, “Entropy and Randomness Online Tester.” [Online]. Available: https://servertest.online/entropy. [Accessed: 25-June-2020].

[23] F. Webster and S. E. Tavares, “On the Design of S-Boxes,” in Advances in Cryptology - CRYPTO ’85 Proceedings, 1986, pp. 523–534.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731