IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. II (Jul.-Aug. 2016), PP 77-81
www.iosrjournals.org

Cuckoo Search based Optimal Elliptic Curve Cryptography (OECC) for Text Encryption

Gnanaprakasam Thangavel[1], Rajivkannan Athiyappan[2]
[1](HoD/CSE, The Kavery Engineering College/Anna University, India)
[2](HoD/CSE, K.S.R. College of Engineering/Anna University, India)

Abstract : *The Cryptography converts our original text information into non understandable form of text that is cipher text which is more powerful because which is not understandable. . In this work we are implemented the text encryption using the Optimal Elliptic Curve Cryptography (OECC) method using Cloud Simulator. Practical results and comparisons of Elliptic Curve Cryptography (ECC) and OECC are presented. The Cuckoo Search (CS) algorithm is used to find the best key as the input of the OECC encryption and decryption process. Using 12 different text documents we generated the encryption time, decryption time comparison. The efficiency of ECC is improved by OECC; finally we found that OECC has more advantages for text encryption and decryption process.*

Keywords : *Cuckoo Search, Decryption, Efficiency, Elliptic Curve Cryptography, Encryption*

I. introduction

Cryptography is the study of secret writing for security purpose. It has two phases namely Encryption and Decryption. Original information to Cipher text is called Encryption and vice versa process is called Decryption. There are two types of cryptography methods available Symmetric and Asymmetric. Symmetric key cryptography sometimes called as Secret Key. In which there is only one key for encryption, the same key is used for decryption. Some Characteristics are, very simple to generate, no need of special properties, randomly generated k-length strings. In asymmetric key cryptography, encryption process is done using public key and in the receiver side the private key is used for decryption. It is also named as Public Key Cryptography. In this method we have two keys Public Key and Private Key. In current research Elliptic Curve Cryptography (ECC) plays a vital role in security. It provides the maximum level of security compared to all other cryptography methods. In our work, we are applying the Cuckoo Search (CS) algorithm for finding the best suitable and secure key. Yang and Deb are the fathers of CS in the year 2009. After that many researchers inspired by CS due to its efficiency in solving optimization problems.

II. survey of literature

2. 1 Research Articles on Cuckoo Search Algorithm

Ali Al-maamari and Fatma A. Omara in 2015 made a task scheduling algorithm have been proposed to the independent task over the Cloud Computing. The proposed algorithm is considered an amalgamation of the PSO algorithm and the Cuckoo search (CS) algorithm; the experimental results show the reduction of the make span and increase the utilization ratio. In 2016 Thuan Thanh Nguyen et al proposed that the CS solved the network topology optimization. In distributed network identify the optimal location and its size is very difficult, using CS they achieved the high performance. Ehsan Teymourian et al in 2016 used Advanced Cuckoo Search algorithm for tackle the capacitated vehicle routing problem. This algorithm enhanced to control the balance between diversification and intensification of the search process. Alexander Teske et al in 2015 detected the faulty nodes in the distributed system of networks. The empirical results reveal that the two cuckoo-based approaches outperformed their competitors in terms of solution quality and spatio-temporal requirements, with Yang and Deb's version achieving notable improvements over Rajabioun.

2.2 Research Articles on Elliptic Curve Cryptography

In 2016 Manish Kumar and Akhlad Iqbal proposed a algorithm for efficient DNA encoding using ECC. The algorithm first encodes the RGB image using DNA encoding followed by asymmetric encryption based on Elliptic Curve Diffie–Hellman Encryption (ECDHE). The proposed algorithm is applied on standard test images for analysis. The analysis is performed on key spaces, key sensitivity, and statistical analysis. In 2015, R. Balasubramanian and Sumit Giri considered the mean value of the product of two real valued multiplicative functions with shifted arguments. That algorithm is the expected number of primes such that a random elliptic curve over rationals has *N* points when reduced over those primes.

III. proposed method

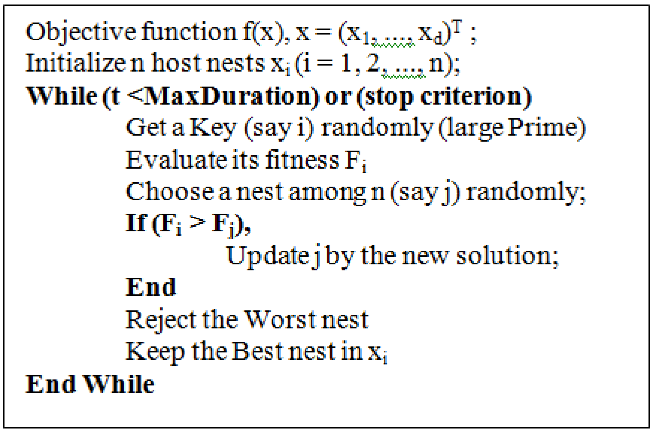
3.1 Cuckoo Search

Cuckoo Search algorithm is inspired by obligate brood parasitism of some cuckoo species by laying their eggs in to the nest of host birds. Those female parasitic cuckoos can imitate the colors and pattern of the eggs of the host species.

The algorithm works on the basis of following three assumptions:

□ □ □ A cuckoo chooses a nest randomly to lay the egg and at a time only one egg is laid by the cuckoo.
2. The best nests with the high quality egg (solution) will carry over to the next generations.
3. The total number of available host nests is fixed and the host bird can discover a cuckoo's egg with a probability,

Procedure 3.1 – Cuckoo Search



```
Objective function f(x), x = (x_1, ...., x_d)^T ;
Initialize n host nests x_i (i = 1, 2, ...., n);
While (t <MaxDuration) or (stop criterion)
    Get a Key (say i) randomly (large Prime)
    Evaluate its fitness F_i
    Choose a nest among n (say j) randomly;
    If (F_i > F_j),
        Update j by the new solution;
    End
    Reject the Worst nest
    Keep the Best nest in x_i
End While
```

3.2 Optimal Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography. For current cryptographic purposes, an *elliptic curve* is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation,

$$y^2 = x^3 + ax + b$$

Key generation is an important part where we have to generate both public key and private key. This private key is generated from the above cuckoo search method. The operations of elliptic curve cryptography are explained over two predetermined fields: Prime field and Binary field. For cryptographic operations the suitable field is selected with finitely massive number of points. The prime field operations choose a prime number, and finitely large numbers of basic points are produced on the elliptic curve.

$$public_{key} = random * CurvePo\,\mathrm{int}$$

Here we optimally select the r values based on the cuckoo search optimization technique.

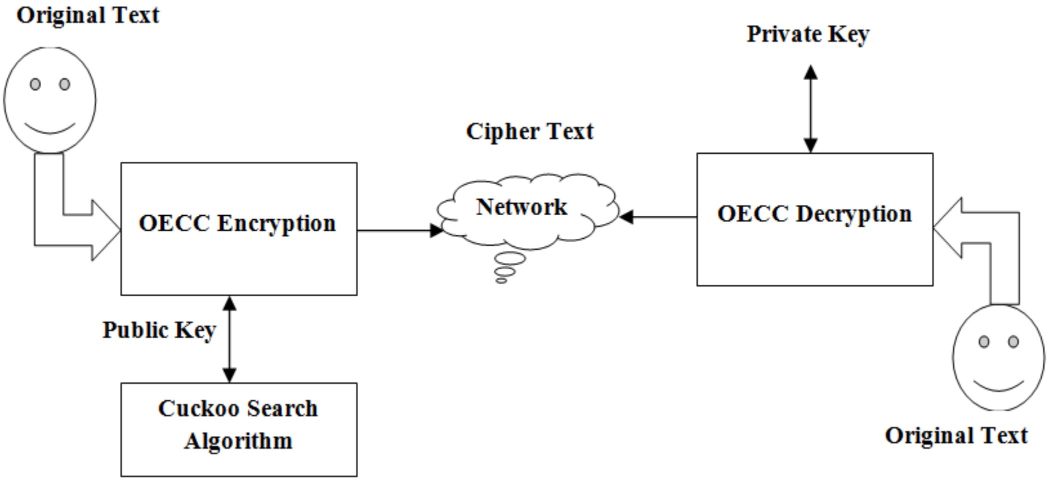


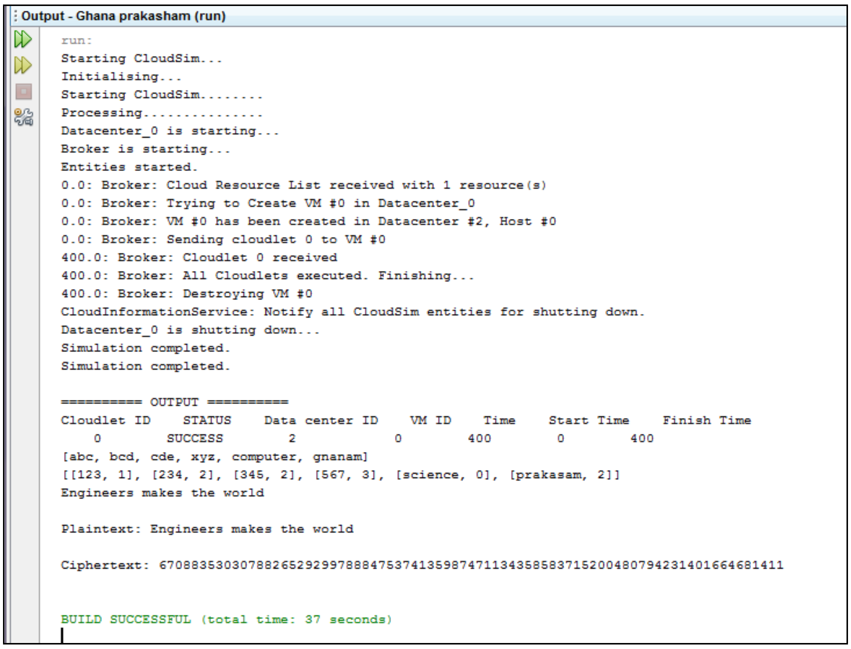
Figure 3.1 Encryption and Decryption Process using OECC

IV. Results and Discussion

4.1 Encryption and Decryption Process

Plain Text: Engineers makes the world

Cipher Text: 67088353030788265292997888475374135987471134358583715200480794231401664681411



```
Output - Ghana prakasham (run)
run:
Starting CloudSim...
Initialising...
Starting CloudSim........
Processing...............
Datacenter_0 is starting...
Broker is starting...
Entities started.
0.0: Broker: Cloud Resource List received with 1 resource(s)
0.0: Broker: Trying to Create VM #0 in Datacenter_0
0.0: Broker: VM #0 has been created in Datacenter #2, Host #0
0.0: Broker: Sending cloudlet 0 to VM #0
400.0: Broker: Cloudlet 0 received
400.0: Broker: All Cloudlets executed. Finishing...
400.0: Broker: Destroying VM #0
CloudInformationService: Notify all CloudSim entities for shutting down.
Datacenter_0 is shutting down...
Simulation completed.
Simulation completed.

========== OUTPUT ==========
Cloudlet ID    STATUS    Data center ID    VM ID    Time    Start Time    Finish Time
    0        SUCCESS        2             0        400        0        400
[abc, bcd, cde, xyz, computer, gnanam]
[[123, 1], [234, 2], [345, 2], [567, 3], [science, 0], [prakasam, 2]]
Engineers makes the world

Plaintext: Engineers makes the world

Ciphertext: 67088353030788265292997888475374135987471134358583715200480794231401664681411


BUILD SUCCESSFUL (total time: 37 seconds)
```

Figure 4.1 Output Screen

For sampling the above encryption and decryption process were shown in Figure 4.1. For 10kb, 20kb, 30kb, 40kb and 50kb files are verified and listed below,

Table 4.1 Performance Comparison

Original File Size (Kb)	Encryption Time (ms)	Decryption Time (ms)
10	0.3	0.2
20	0.35	0.3
30	0.41	0.31
40	0.46	0.36
50	0.62	0.44

Table 4.2 No Information Loss Comparison

Original File Size (Kb)	Encrypted File Size (Kb)	Decrypted File Size (Kb)
10	12.2	10
20	21.5	20
30	32.4	30
40	43.3	40
50	55.1	50

4.2 Encryption and Decryption Time Analysis

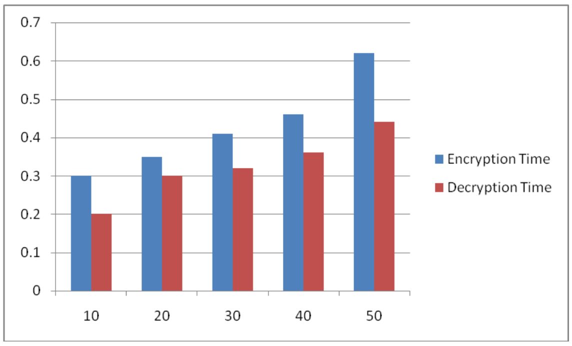


Figure 4.2 Encryption Vs Decryption Time

The above comparison decryption time is lesser than its encryption time, because the key values (Public Key) are taken from the Cuckoo Search process. Even it makes a bit delay, the security aspect its gives the more confidence towards the data.

4.3 No Information Loss

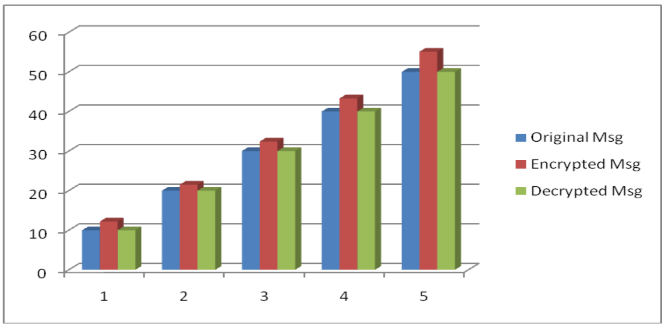


Figure 4.3 Original, Encrypted and Decrypted Message

Even after the encryption process our source file may gets some extra bits (Key) as cipher text file which is not understandable form. But while we decrypt the file, it must not have any additional text or missing information. That we can verify from the above figure 4.3.

4.4 Security Analysis

The best known attack on ECC is Pollard's Rho method and Pollard Lambda method. Pollard's Rho method is expected to find the private key at most a constant time Sqrt[*N*] steps, where *N* is the cyclic order of the Elliptic curve with G as Generator.

Using ECC,

For a 192 bit Elliptic Curve that we have used, *N* value is 6277101735386680763835789423176059013767194773182842284081.

$$\sqrt{NSteps} = 7.92282 * 10^{28}$$

Using OECC,

For a 192 bit Elliptic Curve that we have used, *N* value is 3964531595979731804496592924999053838780170986107576525915854904811453001130

$$\sqrt{NSteps} = 12.4532 * 10^{36}$$

So, OECC gives the best performance in the breaking of keys. The efficiency of the OECC is higher than the ECC process. The Cuckoo Search Algorithm gives the public key as the input of the OECC Encryption process. Hence the key breaking takes more time.

V. Conclusion

This paper investigates the OECC text encryption process and discussed in detail all issues related to encryption time and decryption time, message loss, and key braking time. Due to maintain the confidentiality in the network this model has a promising, prospect in this growing and challenging domain. First the CS algorithm is studied and the usage of better key selection is identified. The selected key is used in the OECC encryption process to increase the key breaking time. The results of encryption and decryption time show that the efficiency of the CS based public key used in effective manner. Information loss is verified in the above results. As far as security concern, the key breaking time is compared with the pollards rho method. There also exists much scope for the future work in the form of Image encryption, Audio/Video encryption methods.

References

Journal Papers:

[1] Thuan Thanh Nguyen, Anh Viet Truong, Tuan Anh Phung, A novel method based on adaptive cuckoo search for optimal network reconfiguration and distributed generation allocation in distribution network, *International Journal of Electrical Power & Energy Systems*, Volume 78, June 2016, Pages 801-815

[2] Ping Jiang, Feng Liu, Jianzhou Wang, Yiliao Song, Cuckoo search-designated fractal interpolation functions with winner combination for estimating missing values in time series, *Applied Mathematical Modelling, In Press, Corrected Proof*, Available online 28 July 2016

[3] Ehsan Teymourian, Vahid Kayvanfar, GH.M. Komaki, M. Zandieh, Enhanced intelligent water drops and cuckoo search algorithms for solving the capacitated vehicle routing problem, *Information Sciences, Volumes 334–335, 20 March 2016, Pages 354-378*

[4] Alexander Teske, Rafael Falcon, Amiya Nayak, Efficient detection of faulty nodes with cuckoo search in *t*-diagnosable systems, *Applied Soft Computing, Volume 29, April 2015, Pages 52-64*

[5] Ali Al-maamari, Fatma A. Omara, Task Scheduling using Hybrid Algorithm in Cloud Computing Environments, *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. VI (May – Jun. 2015), PP 96-106.*

[6] Manish Kumar, Akhlad Iqbal, Pranjal Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography, *Signal Processing, Volume 125, August 2016, Pages 187-202.*

[7] R. Balasubramanian, Sumit Giri, The mean-value of a product of shifted multiplicative functions and the average number of points of elliptic curves, *Journal of Number Theory, Volume 157, December 2015, Pages 37-53.*

[8] Punam V. Maitri, Aruna Verma, Enhancing File Security using Cryptography Algorithms in Cloud Computing: A Survey, *International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 10*, October 2015.

[9] Ikshwansu Nautiyal, Madhu Sharma, Encryption using Elliptic Curve Cryptography using Java as Implementation tool, *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 4, Issue 1, January 2014

[10] C. Nithiya, R. Sridevi, ECC Algorithm & Security in Cloud, *International Journal of Advanced Research in Computer Science & Technology,* Vol. 4, Issue 1 (Jan. - Mar. 2016)

[11] Dr. Chander Kant, Yogesh Sharma, Enhanced Security Architecture for Cloud Data Security, *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 3, Issue 5, May 2013.

[12] Hussain Aljafer, Zaki Malik, Mohammed Alodib, Abdelmounaam Rezgui, A brief overview and an experimental evaluation of data confidentiality measures on the cloud, *Journal of Innovation in Digital Eco Systems 2014.*

[13] Mark D. Ryan, Cloud computing security: The scientific challenge, and a survey of solutions, *The Journal of Systems and Software 86 (2013) 2263– 2268.*

[14] Jingwei Huang and David M Nicol, Trust mechanisms for cloud computing, *Journal of Cloud A Springer Open Journal, Systems and Applications 2013, 2:9*

[15] Dhaval Patel, M.B.Chaudhari, Data Security in Cloud Computing using Digital Signature, *International Journal For Technological Research In Engineering* ,Volume 1, Issue 10, June-2014