Grenze International Journal of Engineering and Technology, Jan Issue

Cipher Block Chaining Technique based on Euler Graph

MPR Murthy[1] and CH. Suneetha[2]
[1]Sr. Assistant professor in Mathematics, GVP college for Degree and PG Courses(A), Visakhapatnam, India
[2]Associate Professor in Mathematics, GITAM University, Visakhapatnam, India
Author for Correspondence: schivuku@gitam.edu

***Abstract*—The present Covid 19 pandemic has created a destruction towards the physical meet and physical talk among the people all over the world. All the communications like social, business, personal including secret are done by using digital techniques. Digitalization has become mandatory for all types of transmissions. Secure communication of secret information has become a hard task due to the extensive growth of wireless networks. It is essential for the service providers to add on extra security level for the messages in their transmission from one place to the other. The task of providing the security is done by encryption technique alone. Applied graph theory plays a crucial role in encryption technique as it has widespread special features equipped with easy and effective representation. The present paper explores a symmetric encryption technique using Eulerian circuits of weighted Euler graphs and simple logical operations.**

***Index Terms*— Euler Graph, Euler Circuit, Encryption, Decryption.**

I. INTRODUCTION

A science of communication of secret information with protection in the presence of a harmful third party is cryptography. In the present era of extensive and thoughtless use of the internet as a basic means of communication creates a threat of hacking and stealing the secret information in the transmission medium. So, concealing the secret information illegible to unauthorized persons is most required aspect in communication network. Graph theory, a major part of applied mathematics has a wide role in the history of cryptography. Many complex problems in our day-to-day life can be represented and solved by graph structures as it provides simple and clear pictorial representation. The flexible properties of graph structures give an additional strength to cryptosystems. The history of cryptography shows diverse graph theory applications in the encryption process. The Relationship between graph theory and cryptography is very interesting.

Graph Theory

Euler's Theory**:**

A connected graph containing a Eulerian circuit is called the Euler graph [1].

Eulerian Circuit**:**

A circuit which touches every edge of the graph exactly one and returns to the same vertex is known as Eulerian circuit. If all the vertices of the graph are of even degree, then the graph is called as Euler Graph.

Euler Path**:**

A graph meeting every edge of the graph and coming back to the same vertex is called the Euler Path.

Grenze ID: 01.GIJET.8.1.8

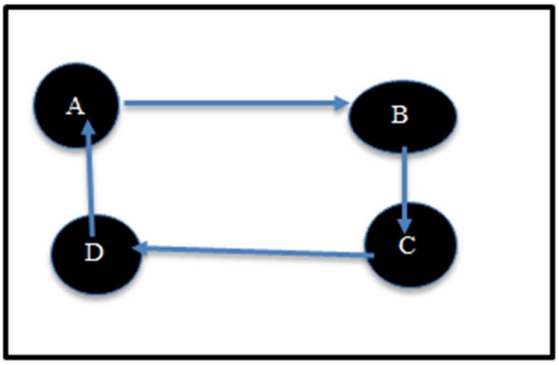


Fig.1

Euler Theorem**:**

- Euler theorem states that if there are more than two vertices, with an odd degree in a graph it does not have a Euler path.
- A connected graph having 0 or exactly two vertices with odd degree contains at least one Euler path and Euler circuit

Obtaining Euler path in a graph**:**

There are two different ways to find the existence of the Euler circuit in a graph:

1. Fleury's Algorithm
2. Eulerizing a graph

Fleury's Algorithm**:**

All the vertices of Euler's graph or circuit are of even degree. This method is erasing the edge after meeting it, from any one of the vertices the travel is started, after finishing the travel at the edge that particular edge is erased until we reach the starting vertex [2].

Eulerizing a graph**:**

It is a process of changing a graph so that it contains a Euler circuit. It is in other words constructing postman or newspaper boy friendly roads in a city to save the mailman's or paper boy's time in delivering the mail or paper. It is a process of identifying and pairing up the vertices with odd degree, keeping average distance as small as possible. All vertices are duplicated along with optimal path.

Euler graph application

Euler graphs have diverse applications in all branches of Science and Engineering like Bioinformatics in CMOS circuits designs to find the optimal logic gates and also to find bridge problems in the field of navigation to find out the optimal feasible solution. They are also used in Game Theory, Floor designs and Chinese postman problems [3].

Euler's Theorem**:** A connected planar graph with P vertices, Q edges has F faces where F
satisfies the solution P - Q + F = 2

Euler's Handshaking Theorem**:** Sum of degrees of vertices of Euler's graph is equal to twice the number of edges of the graph [3].

$\Sigma d\,[V(G)] = 2|e(G)|$

Electronic Code Book**:**

It is a block cipher which supports a separate encryption key for each block.

But ECB mode is deterministic. There is a chance that the same message is encrypted with the same key. ECB mode is further developing cipher block chaining (CBC) mode.

Cipher Block Chaining (CBC**):**

In CBC mode the first block is encrypted with initialization vector the first block cipher is concatenated to second block register for second block encryption. The procedure is repeated for subsequent blocks.

II. Related Work

Graph theory has many applications in cryptography. Graph theory applications are appearing in many branches of cryptography to develop encryption algorithm, key communication technique nowadays. V.A. Ustimenko [4] proposed multivariate cryptography using polynomial maps of affine space over a finite commutative ring into itself as encryption tools. N Tokareva [5] established the relation between graph theory and cryptography. That

paper discusses sparse graphs, Cayley graphs and bent functions applied to mobile networks. Wael Mahmoud Al Etaiwi [6] suggested a new complex cipher basing on cyclic graphs, complete graphs, and minimum spanning tree. Etaiwai technique of graph-based encryption has become more popular referred by many researchers. P. Amudha et.al. [7] surveyed many graph theory applications of cryptography. That chapter proposes an encryption algorithm using Euler graphs. Yamuna et.al [8] suggested a double encryption technique using Hamilton path and complete graph. Steve Lu et.al. [9] proposed applied graph theory to image cryptography by assigning nodes and edges to images. Charles et.al. [10] designed new collision resistant hash functions from expander graphs. AnmariaCostache et.al. [11] studied the security of a proposal for post quantum cryptography using super singular isogeny graphs. Later, Hyungrok Jo [12] introduced cryptographic hash functions based on Charles expander graph in post quantum cryptography. Considering the literature on graph theory applications in cryptography the present paper explains an innovative encryption technique using weighted Euler graph.

III. PROPOSED SCHEME

In the present scheme a weighted Euler graph act as a secret key in communication network. Before communication one of the users publishes a weighted Euler graph with all possible Euler circuit representations or it can be done by a trusted key management authority. A Euler circuit can be drawn in many ways using different vertices of the graph in different directions for instance consider a graph with four vertices ABCD. Euler circuit can be drawn in many ways starting from different vertices of the graph in different directions. For instance, different Euler circuit representations of the same graph are

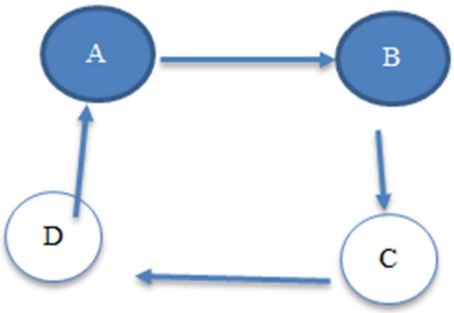


Fig.2 AB-BC-CD-DA

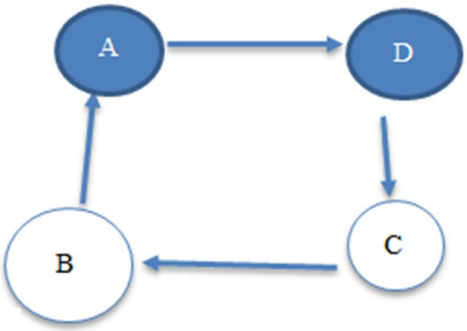


Fig. 3 AD-DC-CB-BA

Similarly

BC-CD-DA-AB
BA-AD-DC-CB
CD-DA-AB-BC
CB-DA-AD-DC
DA-AB-BC-CD
DC-CB-BA-AD

All the Euler circuit representations are given numbers I,II,III,IV,....

Encryption

1.The transferring message or plain text is split into plain text blocks of length equal to the number of edges of the agreed up on Euler graph. All these plain text blocks are given numbers 1,2,3,4.....
The Euler circuit representation I,II,III,IV, ... will act as encryption / decryption keys to the plaintext/ciphertext blocks 1,2,3,4…… consecutively.

2. The character of all the blocks are coded ASCII binary values. The edge weights of Euler circuit representations I,II,III,IV,…… are converted to 8 bit binary numbers. If any edge weights are big numbers more than 256 then the number is reduced to mod 256

3. Logical XOR Operation is performed between ASCII binary values of the characters of first plaintext block and 8bit binary equivalents of the corresponding key. i.e., 8 bit binary equivalents of I Euler circuit representation.

4. For instance if M1(1),M2(1),…….Mn(1) are entries in the first block, E1(I),E2(I),…..En(I) are entries of the first block key then element wise logical XOR operation is performed to yield the first block cipher.

$$Cn(1) = Mn(1) \oplus En(I)$$

n = 1,2,3….. represents the size of the plaintext block as well as key block (Euler circuit representation).
5. First block cipher is concatenated with second block key, to be used as the key for second block encryption.
Kn(II) = Cn(1) ⊕En(II)
n = 1,2,3….. represents the size of the plaintext block as well as key block (Euler circuit representation).
6. The second block elements are encrypted by applying logical XOR between Kn(II) and second plaintext block Mn(2) to get the second ciphertext block Cn(2)
Kn(p) = En(p)
Cn(p) = Mn(p) ⊕Kn(p) for p = 1
Kn(p) = En(p) ⊕ Cn(p-1)
Cn(p) = Mn(p) ⊕Kn(p) for p = 2,3,…… and n = 1,2,3…. represents the size of plaintext or key block. Here p represents the number of
plaintext or key blocks.
7. All the binary elements are coded to ASCII characters and sent to the receiver as cipher text in public medium.
Decryption**:**
At the receiver's end the cipher text is converted into blocks of agreed upon size equal to the size of Euler representations. Since it is symmetric cipher, the decryption is from first block itself.
Mn (1) = Cn(1) ⊕En(I)
Mn(p) = Cn(p) ⊕Kn(p)
Kn(p) = En(p) ⊕ Cn(p-1) for p = 2,3,……and
Kn(p) = En(p) for p = 1

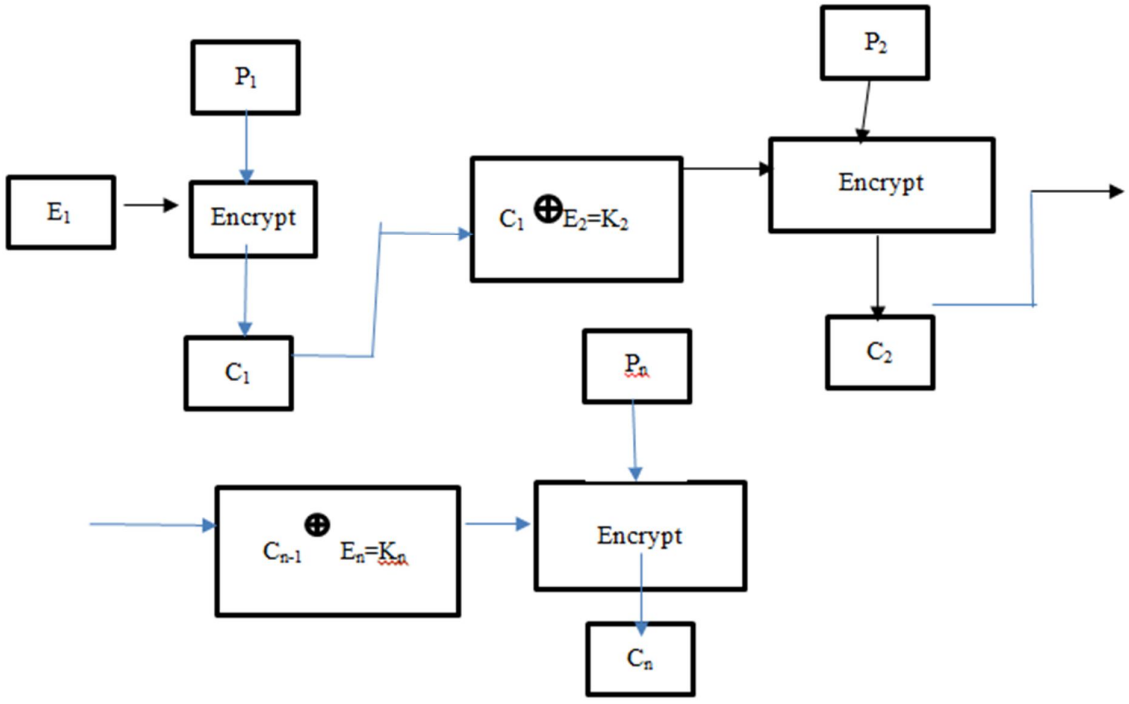


Fig.4

IV. Implementation of the Algorithm

If Alice and Bob want to communicate with each other first, they consider a weighted Euler graph with 12 vertices. It is a Euler graph since each vertex is having even degree.
There are 32 independent Euler circuit representations in the present graph with size 16 decimal numbers each like

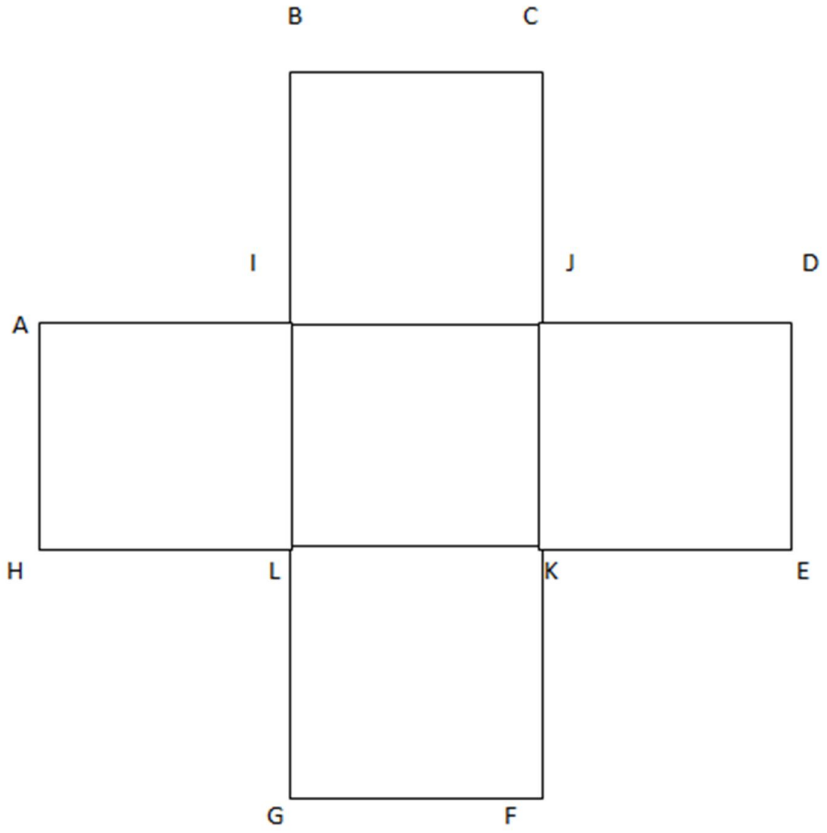


Fig. 5

AI,IB,BC,CJ,JD,DE,EK,KJ,JI,IL,LK,KF,FG,GL,LH,HA with 16 edge weights 18,8,22,29,19,532,13,22,181,14,272,10,46,173,192,94

BI,IA,AH,HL,LG,GF,FK,KL,LI,IJ,JK,KE,ED,DJ,JC,CB with edge weights 8,18,94,192,173,46,10,272,14,181,22,13,532,19,9,22 and so on.

GITAMDEEMEDTOBEUNIVERSITYRUSHIKO/NDAVISAKHAPATNAM530045APINDIA

As the message to be communicated has 32 characters it is divided into two blocks of 16 characters each and the encryption is done by using the above two keys(Euler circuit representations) using chaining mode of first block cipher to the second block key to get the ciphertext

UABJAPSVKT^Ai—vtF[BS -y ∃CDW*ε c*^ \ZUY DC3 SUB J *ϕ*i - VTVT ETB R¬ETB NUL = *μ*

Since there are 32 independent representations with size 16 decimals each, we can encrypt the big message containing 512 characters. By considering the Euler weighted graphs with more of number vertices and edges the proposed scheme can be applied for lengthy messages.

V. Performance Analysis

Etaiwi scheme [2] has become more popular graph-based encryption technique being referred by several researchers in the history. This graph-based encryption scheme used minimal span tree, matrix multiplication algorithms. The execution time of Etawai scheme and the proposed encryption technique are implemented for different sizes of data on Intel core i5, 10^{th} generation processor using MATLABR2011, shown in the following table.

The below table I and graph clearly show that the implementation time is comparatively low in our proposed algorithm. This lowers the computational overhead which is one of the required properties of a good cipher.

Besides the computational overhead Etaiwai scheme possesses broadcast difficulty also. The cipher text size is too big. A plain text with 10 characters is changing into 63 characters cipher text. Cipher size is calculated for different sizes of plaintext, presented in the following table II and graph.

TABLE I

Size of the data in KB	Encryption/Decryption Time in Milliseconds	
	Etaiwi Scheme	Proposed scheme
0.1	169	24
0.2	338	28
0.3	507	30
0.4	674	36
0.5	845	42
0.6	1014	44
0.7	1183	50
0.8	1352	58
0.9	1521	63
1	1691	70

Fig. 6 Execution Time Graph

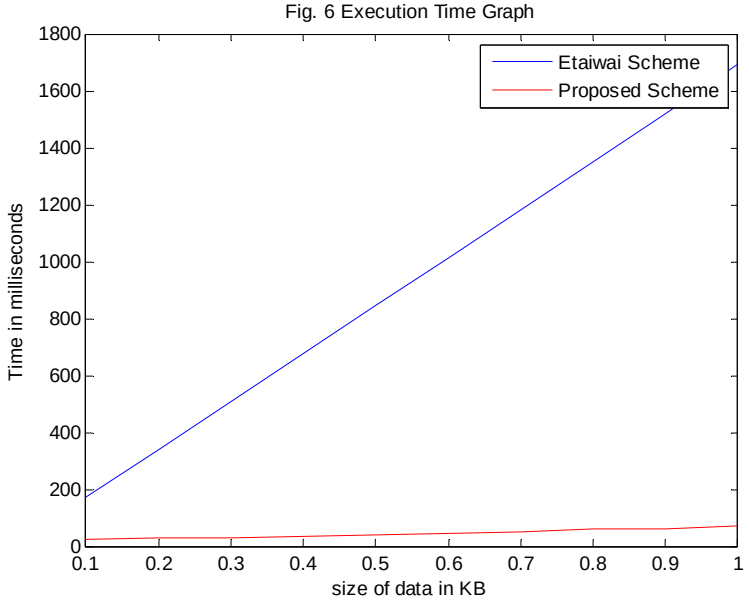
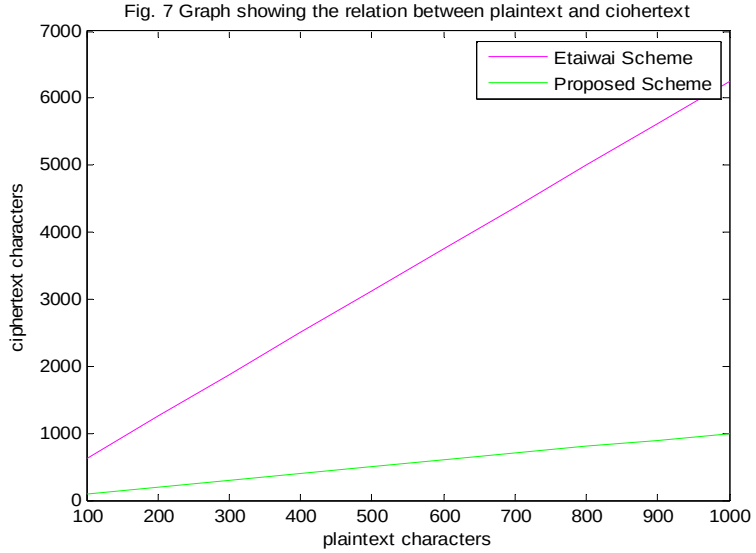


TABLE II

Plaintext characters	Ciphertext characters	
	Etaiwi Scheme	Proposed scheme
100	625	100
200	1250	200
300	1875	300
400	2500	400
500	3125	500
600	3750	600
700	4375	700
800	5002	800
900	5625	900
1000	6250	1000

Fig. 7 Graph showing the relation between plaintext and ciohertext



The above Table.2 and graph in Fig. 7 shows that there is abnormal nonlinearity between sizes plaintext and ciphertext. Even the author has concluded that there may be an improvement for his scheme to decrease the size of the ciphertext. of improving his scheme. One of his suggestions is to divide the whole message into blocks.

VI. Security Analysis and Conclusions

Apart from the good performance the block cipher proposed here achieves best security also. In the proposed scheme a weighted Euler graph with different independent Euler circuit representations is the secret key between communicating parties. Sharing of the secret key is either done by one of the users or by any other trusted external secret key provider agency. Cipher block chaining mode technique is applied from the second block. The scheme uses simple logical XOR operation with concatenation of preceding cipher block to the present block key (Euler circuit representation) to generate a new key for present block encryption. The robustness of the cipher depends on one of the required factors of long and strong key.As the key size of each block is the number of edge weights of Euler graph the length of the key may be enhanced by considering the Euler graph with a greater number of vertices and edges. More the key size more the resistance of the cipher. It is hard against all types of active and passive attacks. As the repeated plaintext characters are mapped to different cipher text characters the present block cipher is free from known plain text analysis linear cryptanalysis. In case if there is same message in two different blocks it is reflected as different cipher text characters as the encryption is done by using different keys for different blocks. This avoids the chosen cipher text attack differential cryptanalysis. So, the present cipher achieves all the required properties of a good encryption algorithm with add on good features low computational overhead and less transport risk with same level of security as conventional graph-based cryptosystems.

References

[1] R. Balakrishnan,K. Ranganathan A Textbook of Graph Theory Second Edition
[2] Narsingh Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice Hall, 2010.
[3] Van Steen M. Graph Theory and Complex Networks: An Introduction. Maarten van Steen. 2010.
[4] V.A. Ustimenko , "On algebraic graph theory and non-bijective multivariate maps in Cryptography", DOI: http://dx.doi.org/10.15439/2018F204
[5] Natalia Tokareva, "Connection between graph theory and cryptography G2C2: Graphs and groups, Cyclic and Coverings, Sep 2014, Novosibirsk Russia.
[6] Wael Mahmoud Al Etaiwi, "Encryption algorithm using graph theory", Journal of scientific research and reports, 3(19) 2519-2527, 2014.
[7] P. Amudha, A.C. Charles Sagayaraj, A.C. shantha Sheela, "An application of graph theory in Cryptography" , International journal of pure and applied mathematics IJPAM, 119(3), 2018, pp 375-383.

[8] Yamuna M, MeenalGogia, Ashish sikka,Md.Jazib Hayat Khan, "Encryption using graph theoryand linear algebra", International journal of computer applications IJCA, 2012.
[9] S Lu, Rafael Ostrovsky, Daniel Manchala, "Visual cryptography on graphs", Cite Seeix COCOON, 2008, 225-234.
[10] Denis X Charles, Eyal Z. Goren, Kristic E. Lauter, "Cryptographic hash functions from expander graphs", Journal of Cryptology, 22, 93-113, 2009.
[11] AnmariaCostache, Brooke Feigon, Kristin Lauter, MaikeMasierer, Anna Puskar, "Ramanujan graphs in cryptography", arXiv:1806. 05709V2 [math.NT]18th December 2018.
[12] Hyungrok Jo, "Ramanujan graphs for post quantum cryptography", http://www.researchgate.net/publication/337150777.