Grenze International Journal of Engineering and Technology, June Issue

Tweakable Block Cipher based on Catalannumber

G. Lalitha Devi[1] and CH. Suneetha[2]
[1]Assistant professor in prism degree college, Visakhapatnam, India
Email: lalithasana07@gmail.com
[2]Associate professor in GITAM University, Visakhapatnam, India
Email: schivuku@gitam.edu

***Abstract*—The present COVID pandemic has transformed a physical world to a digital world. Electronic communication has become a major part of the human life that leads to a threat to digital network. so, hiding and protecting the information against unintended persons is highly essential nowadays. This can be done by encryption process. Encryption techniques are derived from mathematical concepts like number theory, graph theory, and algebra. The present paper explains a tweakable block cipher using Catalan numbers of applied number theory. Here the Catalan number acts as a public key. A cyclic permutation is secret key between the legitimate users that acts as a tweak in encryption process.**

***Index Terms*— Catalan number, Encryption, Decryption, Tweak.**

I. INTRODUCTION

Block cipher uses a pseudorandom permutation (PRP) which is deterministic. As the conventional block ciphers use the same key for all the blocks, they are underlying primitive. Later, for different user applications several modes of operations for block ciphers are developed like Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Offset Code Book mode (OCB) etc. In all these mode message is divided into blocks and encryption algorithm is applied on each block with some agreed upon initialization vector or key.

Enc [M, K] ⟵ Cipher

In conventional block ciphers the sizes of plaintext and cipher text are identical. As the size of the cipher text is deterministic there is no room for integrity of the cipher.

II. TWEAKABLE BLOCK CIPHER

In tweakable block cipher each plain text block is encrypted with the key and with an additional quantity called tweak to yield the cipher text blocks. The tweak is a mathematical quantity which is like the initialization vector used in CBC mode or a nonce in offset code book (OCB) mode [1,8]. The tweak is a vector which can be designed very easily, changed quickly. Sometimes, the tweak can be made public also.

Enc [M, K, T] ⟵ Cipher

A tweakable block cipher has three inputs message or (plain text) M, key K, tweak T and output Cipher text. Since a tweak is frequently changeable, the security of the cipher can be maintained incase when adversary controls input of the tweak.

Grenze ID: 01.GIJET.8.2.508_1

III. Related Work

Moses Liskovet.al [1] proposed the construction of tweakable block ciphers. ChristotBenerle et.al. [2] Developed a lightweight tweakable block cipher with efficient protection against DFA attack. Considering the area footprint of round based hardware implementation.Muzafersaracevic [4] et.al. Proposed cryptographic key generation algorithm of polygon triangulation and Catalan numbers in three phases. Farerkselimovic[5] et.al.applied Delaunay triangulation and Catalan objects in steganography. In that chapter the authors used image encryption techniqueD.Sravankumar et.al.[6] proposed a novel encryption scheme based on catalan numbers. MuzaferSaracevic[7] et.al.suggested method in biometric identification process in application of triangulation combination with face recognition technique.

IV. Applied Number Theory And Catlan Numbers

Applied number theory plays a major role in the history of cryptography. Several cryptographic algorithms were designed using Fibonacci numbers, Lucas numbers and golden numbers [3]. Lucas sequences were applied to improve the Diffie-Hellman key distribution and El Gamal public key. Golden ratio is used in elliptic curve cryptosystems.

V. Integer Sequence

A sequence whose nth term is explicitly given by a relation between the terms is known as integer sequence. Example, Fibonacci sequence 0, 1, 1, 2, 3, 5, 8, 13…. Formed by using the formulae $n^2 - 1$, starting 0 and 1.

VI. Catalan Numbers

Catalan numbers were discovered by a Belgian mathematician Eugene Catalan. It is a sequence of natural numbers denoted by C_n.
The formula for number sequence is

$$C_n = \frac{2n!}{(n-1)!n!} = \frac{1}{n+1}\binom{2n}{n} n \geq 0$$

For example, If n=20 Cn = 6564120420
Catalan number using Euler`s triangulation problem can also be defined as

$$C_0 = 1\ C_1=1 \quad C_n = \frac{4n-2}{n+1} C_{n-1} \quad n\geq 2$$

VII. Ubiquitous Nature Of Catalan Numbers

Like Fibonacci and Lucas numbers Catalan numbers have ubiquitous nature. Catalan sequences have many applications in Combinatorics in finding the number of lattice paths of mountain ranges (Dyck paths), in formation of binary trees, in parenthesizing problem, in abstract algebra and sports. Polygon triangulation and Catalan numbers have several applications in cryptography. They are used to design encryption algorithms, Cryptography key generation algorithms in the history of cryptography.

VIII. Proposed Method

A large natural number n, corresponding Catalan number $C_n$are made public. A cyclic permutation minimum of length (K=5) is secret between the legitimate users of the group. This agreed upon cycle key K acts as a tweak in the encryption process. This cycle can be changed very easily from time to time with low cost of computation.

IX. Different Phases of Working Procedure

1. *I phase (Key generation technique)*

C_n is an integer sequence is divided into different blocks with size K equal to the agreed upon K-cycle.

2. Apply K-cyclic permutation on each block of the Catalan number sequence C_n to yield a new number sequence C_{n1}. The sequence C_n size always may not be equal to the multiples of K. In such a case, the remaining digits those fall at the end of the sequence will keep as they are i.e.., the extra digit are not undergone the permutation.

For instance, if n=30

C_n = 3 8 1 4 9 8 6 5 0 20 9 2 3 0 4
Suppose K=5
C_n is divided into 3 blocks with extra one digit.

3	8	1	4	9		8	6	5	0	2		0	9	2	3	0		4

If the agreed upon cycle 5-cycle is (2 3 5 1 4)

$$\text{Per } [C_n, K] \longleftarrow C_{n1}$$

C_n =

3	8	1	4	9		8	6	5	0	2		0	9	2	3	0		4

C_{n1} =

4	1	9	8	2		0	5	2	6	8		3	2	0	9	0		4

C_{n1} = 4 1 9 8 2 0 5 2 6 8 3 2 0 9 0 4
3. Here the K-cycle acts as a tweak which can be designed easily and can be changed quickly.

Phase Encryption

1. The plain text is divided into blocks with size equal to the length of the Catalan integer sequence C_n, labeled as plain text blocks M_1, M_2,M_3…….
2. 8 bit binary equivalents of first block characters are undergone logical XOR operation with 8 bit binary equivalents of the new Catalan integer sequence C_{n1} to get the first block cipher S_1.

$$E [M1, C_{n1}] \longleftarrow S_1$$

$$\Longrightarrow E [M1, \text{Per } (C_n, K_1)] \longleftarrow S_1$$

$$\Longrightarrow M1 \oplus \text{per } (C_n, K_1)] \longleftarrow S_1$$

3. For the second block, the new Catalan number sequence C_{n2} is obtained by applying permutation as described in the first phase key generation technique but with different cycle. The cyclic permutation for generating C_{n2} from C_n is divided from the agreed upon tweak K-cycle by incrementing 1 to each digit cyclically.
Suppose

l_1	l_2	…….	l_k

K =

l_1+1	l_2+1	…….	l_k+1

K_2 =

For any $l_i = k+1$ then mod k is considered.
4. The second block characters are encrypted like the first block characters applying logical XOR operation between each 8-bit binary equivalent of characters of M_2 and digits of C_{n2} to yield the cipher text block S_2.

$$E (M_2, C_{n2}) \longleftarrow S_2$$

$$M_2 \oplus \text{Per } (C_n, K_2) \longleftarrow S_2$$

5. All the plaintext blocks are undergone encryption with different keys, generated from the tweak K-cycle.

$$E (M_r, Cnr) \longleftarrow S_r$$

$$M_r \oplus \text{Per } (C_n, K_r) \longleftarrow S_r \quad \text{where r = 1, 2, 3……..}$$

All the binary numbers are coded to equivalent ASCII characters sent to receiver as cipher text.

Phase designing the tweak for subsequence block
In deriving K-cycles from the agreed upon tweak [permutation] by incrementing the digits cyclically there is possibility of repeating the same K-cycle. The cycle with K-digits, is identical to the cycle after incrementing each digit K-times.
For instance if K = 5,

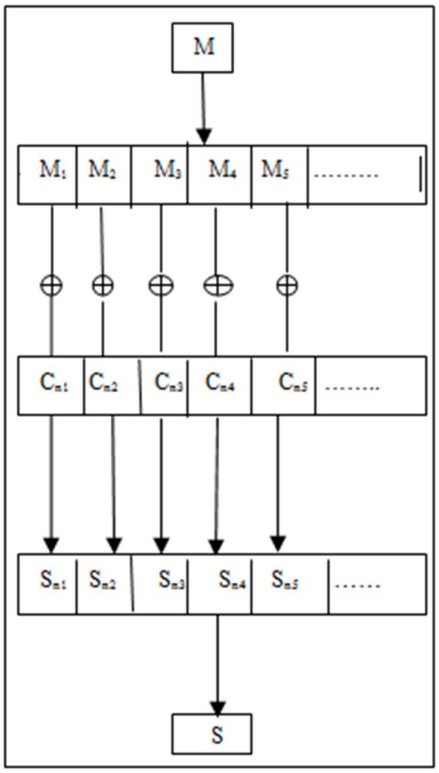

Fig.1

5-cycle = (4 3 5 1 2)

Increment once = (5 4 1 2 3)

Increment twice = (1 5 2 3 4)

Increment three times = (2 1 3 4 5)

Increment four times = (3 2 4 5 1)

Increment five times = (4 3 5 1 2)

So, a 5-cycle when the digits are incremented repeats after 5 steps. So, the encryption key repeats for every I, $(K+1)^{th}$ blocks and. In any case if the same plain text message occurs at I, $(K+1)^{th}$ block; the cipher text also becomes same in those blocks. This gives the room for an adversary to implement different active attacks like linear or differential cryptanalysis. To avoid the unnecessary intervention of the adversary the tweak (agreed upon permutation) is instantly changed when the tweak (cyclic permutation K-cycle) repeats.

X. Instantaneous Change in the Tweak

After getting the repetition of the cycle, the same procedure of incrementing the digits of the agreed upon tweak [K-cycle] by one is implemented but not cyclically. That is the digits of the K-cycle

l_1	l_2	.....	l_k

are incremented by 1 to get the cycle

l_{1+1}	l_{2+1}	.....	l_{k+1}

With this the cycle length becomes (k+1)
Apply K_1 cyclic permutation on full K_1 length blocks of C_n , keeping the partial K_1length blocks as they are, to arrive at new Cn say Cn1.

Example, a 5-cycle is (4 3 5 1 2)
Then the new cycle
K = (4 3 5 1 2)
K_1 = (5 4 6 2 3)
So, now cycle length becomes 6, instead of 5.
K_1 = (5 4 6 2 3)
Now divide Cn into blocks of length 6.

C_{30} = 3 8 1 4 9 8 | 6 5 0 2 0 9 | 2 3 0 4

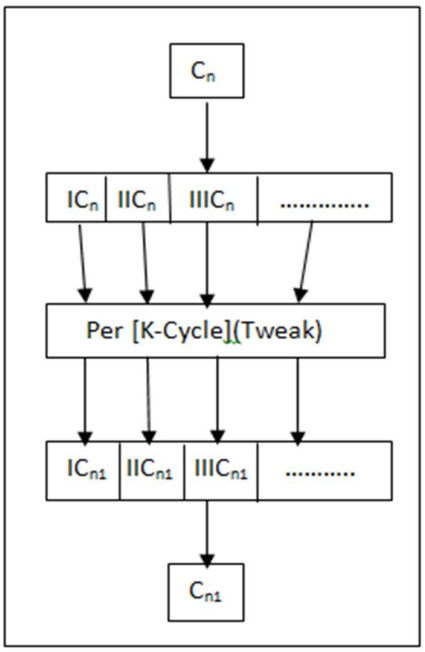

Fig.2

XI. Decryption

Since it is block cipher having symmetric encryption/decryption the receiver after receiving the cipher text divides it into blocks of length equal to length of C_n. Using the agreed upon procedure and tweak the receiver generates block keys C_{n1},$C_{n2...}$…….apply the reverse encryption procedure.

$S_r \oplus Per\ (C_{nr},K_r)$ ⟵ M_r r = 1,2,…….for all blocks

Example-1

Plaintext:

DON`TTAKENEXTAF| TERYOURFIRSTVICT|ORYBECAUSEIF|YOUFAILINSEC|ONDMORELIPSAREWAITING

Cn1 = 498136285002093

Cn2 = 9348108625009243

Cn3 = 398148609520

Cn4 = 384819695002

Cn5 = 386184950220390445231

Cipher text:

pvvQgbssp~ujdxumvfa~ejp{gcdo{wgkasq{wejp{vjwa~ppzx{cuqvr|w|yybaqagu}a{}v

Example 2

Plaintext: GITAMUNIVERSITY| GITAMUNIVERSITY
Cn1 = 8491365280023094
Cn2 = 1349850628030249
Ciphertext: DEL}mp~c{{nubazd`DC1t}nyxex{nuac{``

Computational Information
For n = 30, C_n = 3 8 1 4 9 8 6 5 0 2 0 9 2 3 0 4
K-cycle = 5-cycle = (4 3 5 1 2)
Execution time for Catalan number computation for n=30 is 0.008637sec

XII. Text Encryption/Decryption

Time for loading the Catalan sequence key for n = 30 is 0.008637
Time for tweak application to generate block keys is 0.015799

TABLE I

Text length in characters including spaces	Time in sec
100	0.003809
200	0.004195
300	0.004306
400	0.005123
500	0.004131
600	0.011204
700	0.014711
800	0.006793
900	0.01455
1000	0.01532

XIII. Efficiency Analysis and Conclusions

In the present tweak if block cipher n, corresponding Catalan number may be public or private. The tweak (initialization vector) is secret between the communicating parties. The designing of the tweak is very simple, with low computation time and slightly extra computational cost than the conventional block cipher. In the present given example, the tweak is a 5-cycle, i.e., cyclic permutation vector of length 5. A natural number n, corresponding C_n is the master key, using the tweak the keys for the first, second and subsequent blocks are generated. When the repetition of the K-cycle occurs, the length of the cycle is increased by one unit.i.e., a 5-cycle becomes 6-cycle, then 7-cycle and soon, the tweak can also be changed very easily so that the Catalan number division also changes depending on the length of the new cycle. So, same agreed upon tweak can be maintained for a long time with slight modification. This gives a marginal extra computational overhead and cost rather than rekeying. The basic intention of introducing the tweak [initialization vector] here is both for security purpose and recursive key generation technique.

XIV. Security Analysis

The given two examples show that the cipher is secure against all types of active attacks like linear and differential cryptanalysis. Particularly in the second example, the same plain text message is mapped to different cipher characters due to the reason that the encryption keys are different for different blocks. The proposed tweakable block cipher using Catalan number sequence as key is efficient and secure cryptosystem, in quantum cryptography. Loading the Catalan number sequence, designing the tweak, changing the tweak whenever necessary, generating block keys are simple mathematical techniques with comparatively low computation overhead and less time of execution. So, the present algorithm is a contribution for the application of number theory in Cryptography.

REFERENCES

[1] Liskov, Moses, Ronald L. Rivest, and David Wagner. "Tweakable block ciphers." *Journal of cryptology* (2011), DOI: 10.1007/S00145-010-9073-y

[2] Christof Beierle, Gregor Leander, Amir Moradi,Shahram Rasoolzadeh, "CRAFT: Lightweight Tweakable Block Cipherwith Efficient Protection Against DFA Attacks", https://doi.org/10.13154/tosc.v2019.i1.5-45

[3] El Fadil, Lhoussain "A Public-Key Cryptosystem Based on Lucas Sequences." *Palestine Journal of Mathematics*1.2 (2012)

[4] Anthony over mars, sitalakshmivenkataramanhttps://doi.org/10.3390/mca 23040058

[5] Saracevic, Muzafer, AybeyanSelimi, and Faruk Selimovic. "Generation of cryptographic keys with algorithm of polygon triangulation and Catalan numbers."https://doi.org/10.7494/CSCI

[6] Selimović, Faruk, Predrag Stanimirović, MuzaferSaračević, and Predrag Krtolica"Application ofDelaunay Triangulation and Catalan Objects in Steganography."https://doi.org/10.3390/math111172

[7] D. SravanaKumar, C. H. Suneetha, and A. Chandrasekhar. "Novel encryption schemes based on Catalan numbers." *International Journal of Engineering Research and Applications (IJERA)* vol.2, Issue-2 mar-apr 2012, 161-166

[8] Saračevič, Muzafer, Mohamed Elhoseny, AybeyanSelimi, and Zoran Lončeravič. "Possibilities of applying the triangulation method in the biometric identification

[9] Chakraborty, Debrup, and Palash Sarkar. "A general construction of tweakable block ciphers and different modes of operations." In *International Conference on Information Security and Cryptology*, pp. 88-102. Springer, Berlin, Heidelberg, 2006.