Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

CLEFIA- A Encryption Algorithm using Novel S-Box Architecture

Manjushree B Somasagar[1]
Electronics and Communication Engineering
BMS College of Engineering
Bengaluru, India

Dr. Kiran Bailey[2]
Assistant Professor, Department of ECE
BMS College of Engineering
Bengaluru, India

***Abstract*—Lightweight cryptography is a class in cryptography that is employed in resource constrained devices like embedded systems to provide security. CLEFIA is one of the light weight cryptography algorithms which suits the resource constrained environments in providing security thus enhancing the privacy.**

Keywords—Light weight cryptography; CLEFIA; Composite Field Appoach (CFA); Algebraic Normal Form (ANF)

I. INTRODUCTION

In today’s world as there is too much dependence on Internet of Things (IoT) for daily activities, there is a necessity to provide security in the operation that these perform. The IoT is comprised of resource constrained devices like sensors, embedded systems, RFID tags etc. These do not possess much of the resources so the security functions also need to be incorporated in them along with their intended purpose. The classical encryption algorithms are suitable in computer systems but in the resource constrained environments newly developed class of algorithms called light weight ciphers are used which provide security as well as consume less resources [4].

CLEFIA is one such light weight cipher invented by Sony Corporation. This was originally used to give security in resource constrained environment. CLEFIA was developed in 2007[3][6].

II. RELATED WORK

In order to provide the security the original message signal called the plain text has to be transformed into another form called cipher text. The main intention of changing the plain text is because the original message must not be accessible for the attackers.

The method involved in transforming the plain text to cipher text uses many transpositions and substitutions so that it is protected from the attack.

There are different kinds of algorithms defined based on various characteristics. Among all of them the classification based on keys used in the algorithm is widely used. A single key is employed for the encryption and decryption process in the case of secret key cryptography. Two different keys where one used for encryption and the other one for decryption are considered in case of public key cryptography. There is another class of cryptography where mathematical substitutions are used. This type of cryptography is called as hash functions [2].

Many algorithms are defined to perform the encryption process. The algorithms will consider the Fiestel structures in case of block ciphers. This structure will be involved to perform the substitutions and transformations required in the process. The S-boxes are employed where this is the first stage of creating the confusions.

The key generating blocks is another step in the encryption algorithm. There are many ways in the generation process. The key will be generated and will be combined with plain texts. There are specific numbers of rounds in the process according to the number of bits in the plain texts and the algorithm defined.

III. PROPOSED WORK

CLEFIA one of the light weight block ciphers is implemented. The algorithm is a block cipher which has a bit length of 128 bits. This comprises of variable key lengths with respect to the bit lengths considered. The number of rounds employed in the algorithm succumbs to the key lengths. For a 128 bit plain text there has to be 18 rounds, for a 192 bit length of plain text the number of rounds are 22. And for the 256 bit length of the original message 26 rounds have to be performed. There are 2 S-boxes employed namely S0 and S1 with the F-functions namely F0 and F1. This algorithm consists of round keys and also whitening keys in the process of the algorithm.

A. Architecture of CLEFIA

The CLEFIA that is implemented in our work has been considered to take into account 128-bit length of plain text at a time and the key which is of 128-bit in length. The plain text which is of 128-bit is decomposed to 4, 32-bit chunks namely P0, P1, P2 and P3. The whitening keys WK0 and WK1 are ex-ored with the plain texts P1 and P3. The conversion of the plain text into cipher text happens using the GFN structures. The GFN structures use the F0 and F1 where each F-function uses the round keys RK_i and RK_{i+1}. The sub-blocks used to implement the CLEFIA algorithm are illustrated below [1].

B. S-boxes design

S0 and S1 are the two boxes which are used in CLEFIA. Let us study the details of both these.

S0 box- The implementation of this comprises of using other sub boxes termed as SS0, SS1, SS2 and SS3. These are random boxes. These are combined using the Galois field multiplier [1][3][7]. The lookup table where the S0 values are defined in predefined tables is the most common way of implementing the S0 boxes. But here we have employed the Algebraic Normal Form (ANF) approach.

The SS0, SS1, SS2 and SS3 are basically formulated using ANF expression and gates are used to represent it[1]. This is advantageous compared to former technique as it gives the algebraic degree and linearity of the function.

S1 box- The process of designing the S1 box is done using the Galois Field (2^8) inversion process. The polynomial deployed to implement the S1 box is $z^8+z^4+z^3+z^2+1$. The technique in order to introduce the novelty in the design, we have used the Composite Field Approach (CFA)[1].

b= g (f (a) $^{-1}$) if f (a) /= 0
b= g (0) if f (a) = 0
In the above equation b and a represents S-box output and input respectively.

C. F0 and F1 designs

The F0 and F1 functions are defined using the 4 branch Generalized Fiestel Network (GFN) rather than the conventional 2 branch structure which has an advantage [3]. Due to the 4-branch structure the F0 and F1 function are smaller compared with 2 branch structures which need double the size of input of 4-branch structure. The F-functions consists of the S0 and S1 boxes in addition to 4x4 diffusion matrices. After each round in the F-function the circular shift operation is performed.

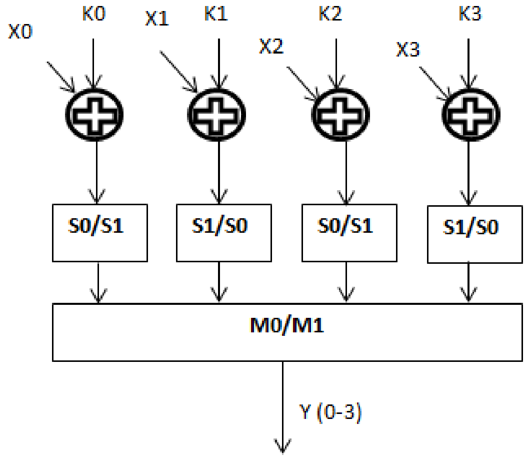

Figure. 1. F-functions

D. Diffusion Matrices

The diffusion matrices namely M0 and M1 are contemplated for the generation of F-functions. The multiplication factors of 2, 4, 6, 8 and 10 are multiplied with the outputs obtained in the S-boxes. These multiplication factors are combined using the xor operation.

E. Key scheduling block

The key scheduling block is designed using a technique called double swap. A 128 bit long word is split as 2, 57 bits and 2, 7 bits [5][6]. Then the swapping takes place in the further step by interchanging the positions of the considered bits. The key scheduling part is developed in order to provide the whitening keys and round keys for the encryption technique. This method of generation uses the K key and an intermediate key I as the first step. The generation of the intermediate key I is done from the Key K. Then the expansion of the keys is performed. The intermediate key I is generated using the GFN structure. This GFN structure is used in the key generation block also. The intermediate key generation is done by applying the key and the 24 bit constant values to the GFN structure. The rest 36 bit values generated are employed to give the keys needed for the encryption process.

IV. RESULTS AND DISCUSSION

The CLEFIA encryption algorithm is developed by using all the sub-blocks designed. The top-level design for the encryption is designed. The simulation of the design is carried out in Xilinx ISE Suite.

For the overall design of the algorithm an intermediate encryption register is deployed to hold the data after each round and the use this as an input for the further rounds. The F0 and F1 functions are used in parallel where the association of the S0 and S1 differs. A multiplexer is involved to take in the input after the rounds based on a signal. The shifting of the data takes place after each round. This can be left/right shift. The encrypted results are obtained.

A. Simulation results

The results obtained after implementing the S-boxes is depicted in Fig. 2.

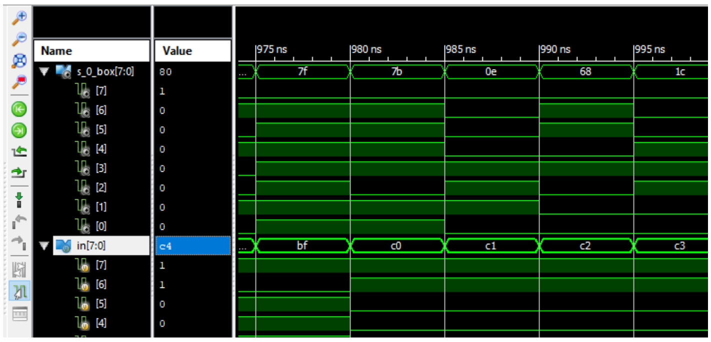

Fig. 2. Output of S0 box

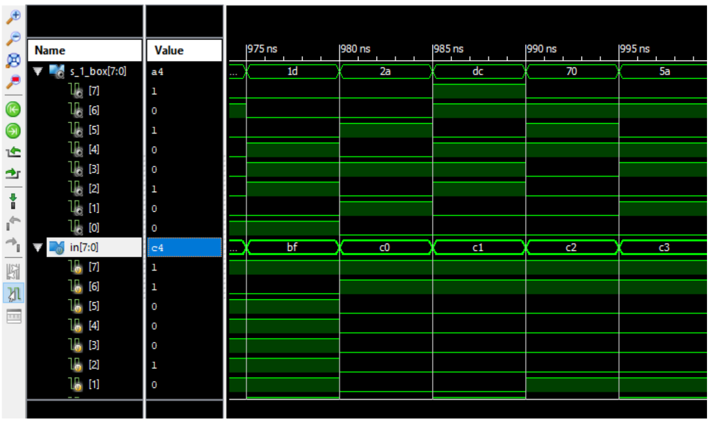

Fig. 3. Output of S1 box

The below table shows the results obtained using the novel approaches used. The total delay in the designs is minimal.

TABLE I. RESULTS TABLE

Approach	***Total delay***
S0 using ANF approach	3.1ns
S1 using CFA approach	4.83ns

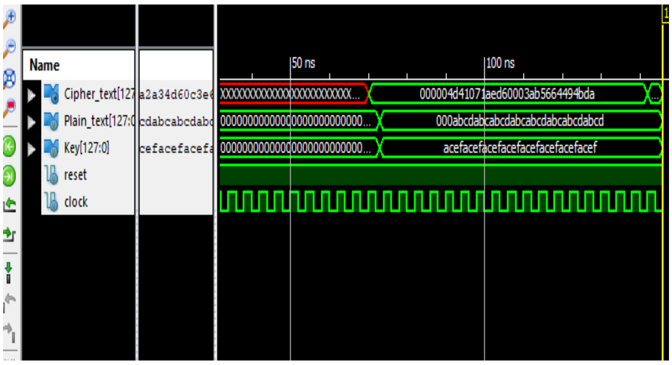

Fig. 4. Output of encryption

The encrypted output of the CLEFIA algorithm is as shown in Fig. 4. The total encryption is accounted within 18 clock cycles.

V. CONCLUSION

The CLEFIA encryption algorithm implemented can be used for the resource constrained devices. This gives a good tradeoff between speed and memory requirement. The novel sub-blocks are integrated at the top level and the implementation results are obtained. This suits the new class of light weight cryptography.

ACKNOWLEDGMENT

I sincerely thank Dr. Kiran Bailey for her guidance and support. I thank her heartfully for her immense support and knowledge sharing. I also thank the BMS College for the support.

REFERENCES

[1] P. Saravanan, S. Subha Rani and H.S. Jatana " An Efficient ASIC Implementation of CLEFIA Encryption/Decryption Algorithm With Novel S-Box Architectures" IEEE transactions on very large scale integration (VLSI) systems 12, no. 9 2019.

[2] CRYPTREC, "Cryptographic Technology Guideline". Available at http://www.cryptrec.go.jp/report/cryptrec-rp-2000-2017.pdf.

[3] Shirai, Taizo, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. "The 128-bit blockcipher CLEFIA." In International Workshop on Fast Software Encryption, pp. 181-195. Springer, Berlin, Heidelberg, 2007.

[4] ISO, ISO/IEC 29192-2:2012, Information Technology - Security Techniques - Lightweight Cryptography - Part 2: Block Ciphers, 2012,Available at : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56552

[5] Sony Corporation, "The 128-bit Block Cipher CLEFIA Security and Performance Evaluations," Jun. 2007, http://www.sony.co.jp/Products/clefia/technical/data/clefia-eval-1.0.pdf.

[6] Sugawara, Takeshi, Naofumi Homma, Takafumi Aoki, and Akashi Satoh. "High-performance ASIC Implementations of the 128-bit Block Cipher CLEFIA." In 2008 IEEE International Symposium on Circuits and Systems, pp. 2925-2928. IEEE, 2008.

[7] Akishita, Toru, and Harunaga Hiwatari. "Very compact hardware implementations of the block cipher CLEFIA." In International Workshop on Selected Areas in Cryptography, pp. 278-292. Springer, Berlin, Heidelberg, 2011.