International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 5, Issue 9, September 2016 **ISSN 2319 - 4847**

Performance analysis of FPGA implementation of enhanced Two-fish encryption algorithm

[1]Dr.G.GEETHARAMANI, [2]P.RAMADEVI

[1]Department of Mathematics
Bharathidasan Institute of Technology Tiruchirappalli -620024

[2]Department of Electronics and Communication Engineering
Bharathidsan Institute of Technology Tiruchirappalli -620024

ABSTRACT

In our latest data transmission and transportation, secured communications is most important task. The task can be achieved by incorporating proper encryption method which provides a fine solution. The encryption algorithm is the mathematical procedure performed on message. To cipher a message and to decipher it back to the original message is called encryption. The key is used for encryption process. Two-fish is one of the symmetric encryption algorithms and it is a strongest algorithm since it has large key stream and number of rounds. The encryption/decryption process is formatted using assortment security key levels to improve the performance of two-fish algorithm significantly. The various set of keys is achieved by using fuzzy logic. The performance of enhanced two-fish algorithm is analyzed by using FPGA implementation.

Key words: Two-fish, Fuzzy Logic Controller, Network Connectivity, Key Generation, FPGA.

1. INTRODUCTION

1.1 Two-fish Encryption algorithm.

Two-fish technique is a 128-bit cipher which includes the implementations of all features like sub-key generation, encryption and decryption that supports keys of length of 128, 192 or 256-bits. In AES-Advanced Encryption Standard rivalry detained by National Institute of Standards and Technology (NIST) the Two-fish scheme is placed as one among five best techniques. The AES system is developed from DES which is an older algorithm. Two-fish is a successor to Blowfish, a well-established cipher and it is more efficient than DES. The hardware implementation is designed and mapped effectively with hardware devices like FPGAs. This paper will describe the implementation of the enhanced Two-fish cipher concept with outstanding achieved results and performances. The section one emphases the detailed information of the structure of cipher's systems as base works. In connection with that the requirement for the design of fuzzy logic controller and different blocks are explained to get final structure to obtain by integration after of all components. The final summary of work details of the incorporated scheme results and performances are explained in detailed way.

1.2 Fuzzy logic control

It is very difficult to design and derive a suitable Fuzzy system for uncertain reasoning, especially for a mathematical model. The decision making along with the estimated values of the incomplete or uncertain information can be allowed by Fuzzy logic systems. A methodical way to incorporate human practice in key generation control is provided by Fuzzy logic control. From the practical experience, the control rules are normally taken out, which may make the result rather subjective and fully relies on the qualitative knowledge of process behavior from that a very good response, is achieved. This paper describes FPGA realization of an enhanced encryption algorithm using Fuzzy Logic Controller (FLC). A fuzzy system improves the relative performance of a key generation in encryption algorithm.

2. EXISTING METHOD

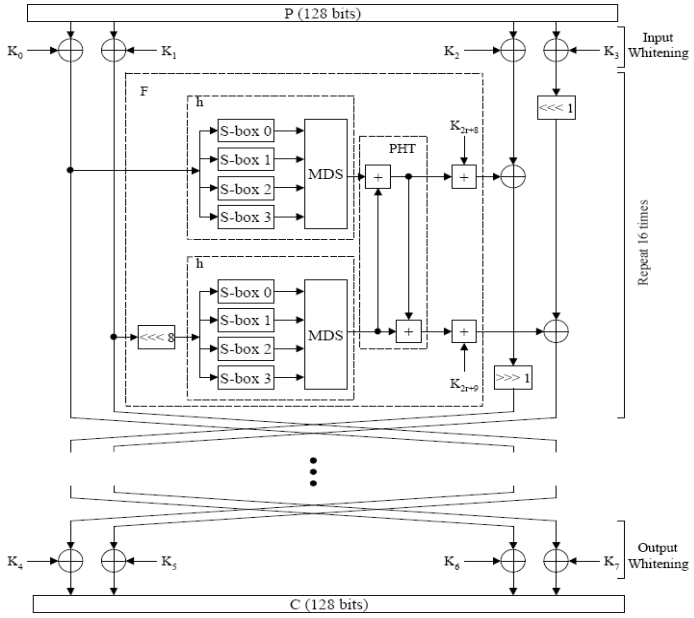

Figure 1- Two-fish Architecture

Overview of Two-fish construction details are exhibits in figure 1. The inputs are initially connected to a register. Then it is estranged into four words which are XOR-ed with four sub keys K0…K3. This process is called input whitening. These estranged data are goes through a module called the F-function where a variety of rotations, transformations and permutations are useful to it. This F-function is accumulation of two h-functions containing key-dependant S-boxes, MDS-Maximum Distance Separable matrices and a PHT-Pseudo-Hadamard Transform. After execution of 16 times using function, the four words of data are another time XOR-ed with four sub keys K4…K7. This step is called the output whitening. To end with, the output register contains the encrypted or decrypted data which are latched.

STEP BY STEP PROCESS

Design decisions for Implementation

i. Q-permutations
ii. S-boxes
iii. MDS matrix
iv. RS matrix
v. PHT transformation
vi. Sub key generation module
vii. Operation selector

3. RESULTS OF EXISTING METHOD

3.1 RTL Schematic view of two-fish

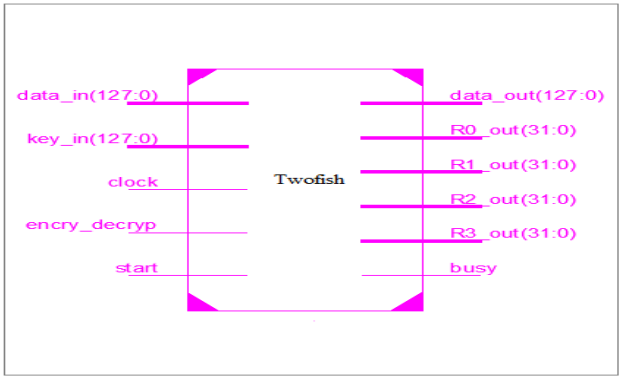

Figure 2 - RTL Schematic view of two-fish

3.2 Encryption results of twofish

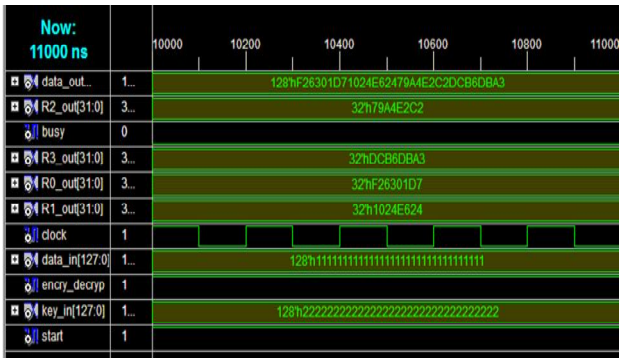

Figure 3 - Encryption results of twofish

4. OBJECTIVE OF THE ENHANCED TWO-FISH ALGORITHM.

The performance of the existing TF encryption algorithm is to be improved by introducing soft computing technique in VLSI platform to achieve the different security level by means of choose the desired key strength depending on our requirement.

5. PROPOSED METHOD

5.1 Methodology

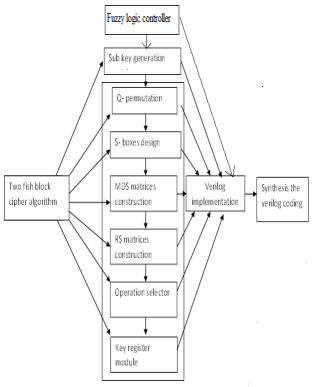

Figure 5 - Flow diagram of enhanced TF

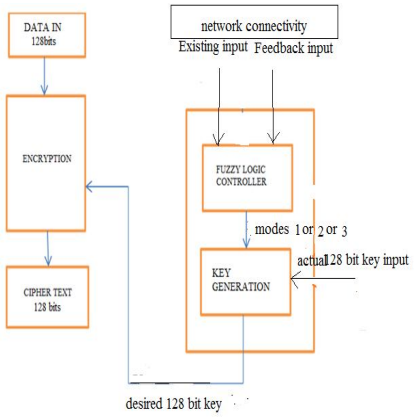

Figure 6 - Block diagram of enhanced TF

Fuzzy logic provides a simple way to arrive at a definite conclusion. The decision making can be achieved from fuzzy logic rules and sets of membership functions. To achieve different security level the algorithm uses desired key. The desired key is obtained using an artificial intelligence called FLC.This proposed work involves the realisation of two-fish encryption algorithm using FLC in verilog HDL. The Fuzzification,Interference and Defuzzification are main blocks in FLC design. Fuzzification is having the process of converting crisp data into fuzzy data or Membership Functions (MFs) according to the logic functions of the system. To derive the fuzzy output Fuzzy Inference Process is being done by combine membership functions with the control rules. Defuzzification the insisted the process to calculate altered methods each connected output in and put a lookup table. Depends upon the application process the data picked up the output from the lookup table based on the current input and convert fuzzy data in to crisp data.

5.2 Membership Functions

The crisp variables are converted into linguistic variables with a process called fuzzification. Five different ranges the input and output variables are divided and each range corresponds to a linguistic variable. The FLC membership functions are getting a value over the range of input and output available variable values and universe of discourse linguistically describes the variables. The linguistic label very Low, Low, medium, strong, very strong (key strength) are triangular input membership functions. The triangle membership functions, the left and right half was chosen to provide for each linguistic label membership overlap with adjacent membership functions. Another membership functions for the labels very Low, Low, medium, strong, very strong (connectivity) are defined.

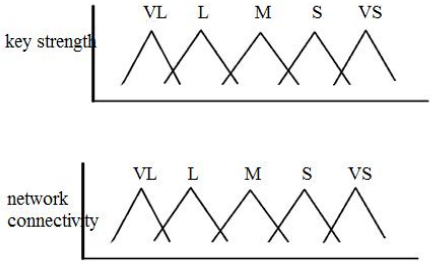

Figure 7 - Membership Functions

VL – very Low
L – Low
M – Medium
S – Strong
VS – Very Strong

5.3 Rule Development

The rule table is prepared which is based on the expert's knowledge. This rule base is the backbone of this system according to which the desired key generated from actual key. Fuzzy logic rules implemented in the form of IF-THEN statements, in this statement the "antecedent" is IF part and the THEN part as "consequent". The modes of operations derived from 25 rules are obtained from rule development table contains network connectivity and key strength.

Table 1 - Rule development table

XY	VL	L	M	S	VS
VL	2	2	3	3	3
L	2	1	2	3	2
M	2	2	2	3	2
S	1	1	2	2	2
VS	1	1	2	2	2

X – Key strength
Y – Network connectivity

5.4 Modes of Operations

The given key of size 128 bit is split into 16 eight bits and modes of operation is performed. There are three modes of operation based on its priority. The modes are

1. Bit cross over 2. Bit swapping 3. Bit flipping

Mode 1: Bit cross over - The middle four bits of the given fuzzifier output is ROR by one bit.
Mode 2: Bit swapping - The given 8 bit is split into two 4 bits and then it is swapped.
Mode 3: Bit flipping - The key of 128 bit is checked consecutively one after the other for three continuous ones. If it is present then the upcoming fourth bit is complemented. Then the same process is done for the all the remaining bits.

Set of 25 rules

If connectivity is very Strong and key strength is very Strong, then mode = 2,
Else if the connectivity is very Strong and key strength is Strong, then the mode = 2,
Else if the connectivity is very Strong and key strength is medium, then the mode = 3,
Else if the connectivity is very Strong key strength is Low, then the mode = 3,
Else if the connectivity is very Strong and key strength is very Low, then the mode = 3,
Else if the connectivity is Strong and key strength is very Strong, then the mode = 2,
Else if the connectivity is Strong and key strength is Strong, then the mode = 1,
Else if the connectivity is Strong and key strength is medium, then the mode = 2,
Else if the connectivity is Strong key strength is Low, then the mode = 3,
Else if the connectivity is very Strong and key strength is very Low, then the mode = 2,
Else if the connectivity is very Low and key strength is very Low, then the mode = 2,

5.5 Results of Proposed method

5.5.1 RTL Schematic view of enhanced two-fish algorithm

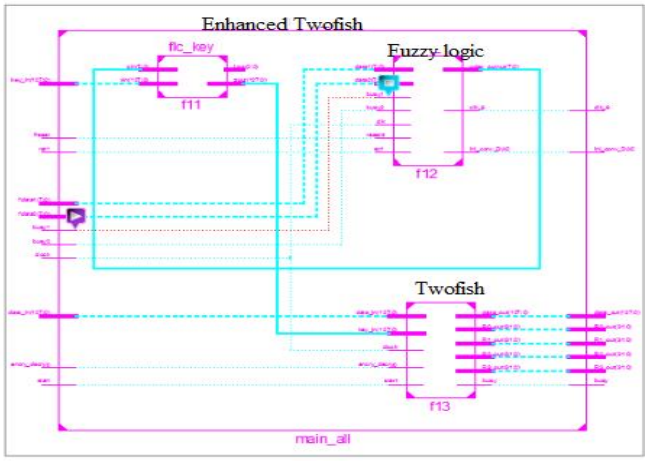

Figure 8 - RTL Schematic view of enhanced two-fish algorithm

5.5.2 Encryption results of enhanced two-fish

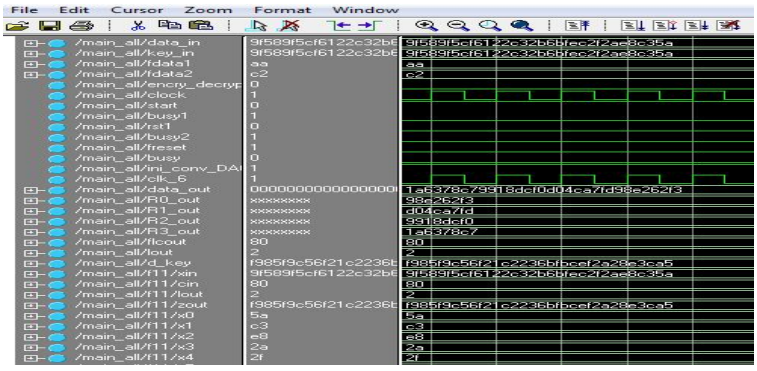

Figure 9 - Encryption results of enhanced two-fish

5.5.3 Decryption results of enhanced two-fish

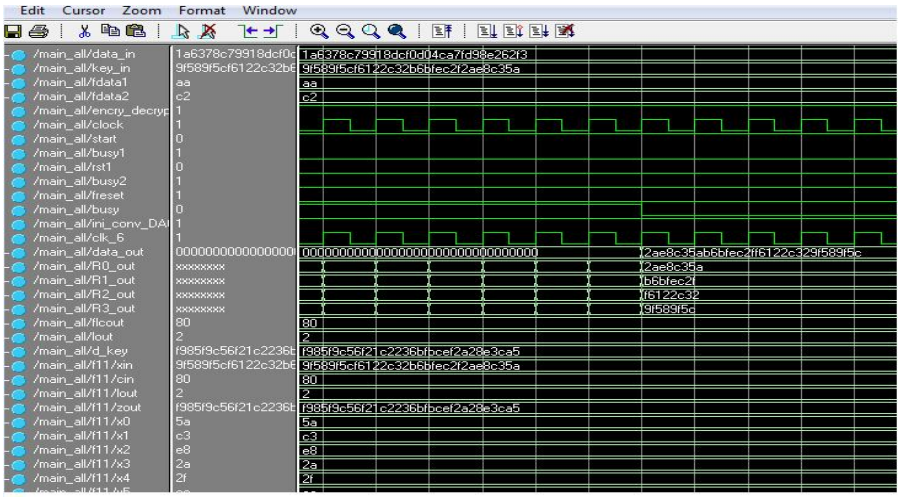

Figure 10- Decryption results of enhanced two-fish

6. Conclusions

The information security can be easily achieved by using Cryptography technique. To protect our confidential communicated data from the hackers a hefty numeral of encryption algorithms have been implemented. But some algorithms have been broken by using Cryptanalysis method. A key is the strongest point of any algorithm but it can become the weakest point if it is not secured. In order to enhance the security of the key, an artificial intelligence called fuzzy logic is used in the key generation block so that key is strengthen to desired key based on the users requirement and data is secured which is performed in the two-fish encryption algorithm. In this paper, two-fish encryption algorithm using fuzzy logic controller is simulated and analyzed by using xilinx ISE 9.21 tool.

References

[1] Pawel Chodowiec, Kris Gaj pchodowi@gmu.edu, kgaj@gmu.edu Technical Report Electrical and Computer EngineeringmGeorge Mason University, "Implementation of the Twofish Cipher Using FPGA Devices", July 1999

[2] Rabie A. Mahmoud1, Magdy Saeb2 1. General Organization of Remote Sensing (GORS), Damascus, Syria. rabiemah@yahoo.com 2. Computer Engineering Department, Arab Academy for Science, Tech. & Maritime Transport (AAST), Alexandria, Egypt. mail@magdysaeb.net , "A Metamorphic-Enhanced Twofish Block Cipher And Associated FPGA Implementation", The International Journal of Computer Science and Communication Security (IJCSCS), Volume 2, January 2012

[3] MarkkuSuni, Sampo Insurance Company, Turku, Finland, "Fuzzy Logic and SAS@ Software - Do They Work Together?"

[4] Purnima Gehlot MITS University, Laxmangarh (Raj.) S. R Biradar MITS University, Laxmangarh (Raj.) B. P. Singh MITS University, Laxmangarh (Raj.), "Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL", International Journal of Computer Applications (0975 – 8887) Volume 70– No.13, May 2013

[5] Mr. Anil G. Bansode, 2Prof.S.O.Rajankar and 3Dr.M.G.Ghatule Sinhgad College of Engineering, Pune, India, "Design and development of smart automatic windshield wiper system: fuzzy logic approach", RESEARCH UINVENTY: International Journal of Engineering and Science ISSN: 2278- 4721, Vol. 1, Issue 1 (Aug2012), PP 14-20 www.researchinventy.com

[6] Gayathri, A. and P. Narayanasamy Department of Information Science and Technology, Anna University, Chennai-25, Tamilnadu, India, "Security in MANET's by Using Detective Signature Techniques", Journal of computer Science. This open access article is distributed under a Creative Commons Attribution (CC-BY) 3.0 license.2015.

[7] Purnima Gehlot MITS University, Laxmangarh (Raj.) S. R Biradar MITS University, Laxmangarh (Raj.) B. P. Singh MITS University, Laxmangarh (Raj.), "Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL ", International Journal of Computer Applications (0975 – 8887) Volume 70– No.13, May 2013

[8] Pawel Chodowiec, Kris Gaj pchodowi@gmu.edu, kgaj@gmu.edu, "Implementation of the Twofish Cipher Using FPGA Devices", Technical Report Electrical and Computer Engineering George Mason University, July 1999.

[9] VekariyaMeghna M.E.(C.E.), B.V.M.Engineering College, V V Nagar, "Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms", International Journal of Computer Engineering and Science, August- 2014

[10] P. Ramanathan, Department of EEE, Bharath University, India. "Fuzzy Logic Controller for Temperature Regulation Process ", Middle-East Journal of Scientific Research 20 (11): 1524-1528, 2014 ISSN 1990-9233 © IDOSI Publications, 2014 DOI: 10.5829/idosi.mejsr.2014.20.11.114162

[11] Mr. Anil G. Bansode, 2Prof.S.O.Rajankar and 3Dr.M.G.Ghatule Sinhgad College of Engineering, Pune, India, "Design and development of smart automatic windshield wiper system: fuzzy logic approach", International Journal of Engineering and Science ISSN: 2278-4721, Vol. 1, Issue 1 (Aug2012), PP 14-20 www.researchinventy.com

[12] Dr.S.S.Dhenakaran, M.Sc., M.Phil., Ph.D, N.Kavinilavu Associate Professor Research Scholar Dept of Computer Science & Engg Dept of Computer Science& Engg Alagappa University Alagappa University Karaikudi karaikudi. "A NEW METHOD FOR ENCRYPTION USING FUZZY SET THEORY", International Journal of Engineering Trends and Technology- Volume3Issue3- 2012 ISSN: 2231-5381 http://www.internationaljournalssrg.org

[13] Ayushi Lecturer, Hindu College of EngineeringH.No:438, sec-12, sonipat, Haryana, "A Symmetric Key Cryptographic Algorithm", ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15

[14]Ravindu Madanayake , Nikila Peiris , Gayan Ranaweera and Uthpala Jayathilake 4 Sri Lanka Institute of Information Technology, Sri Lanka, "Advanced Encryption Algorithm Using Fuzzy Logic" International Conference on Information and Computer Networks (ICICN 2012) IPCSIT vol. 27 (2012) © (2012) IACSIT Press, Singapore.

AUTHER

Dr.G.Geetharamani is working as Associate Professor in Anna University – BIT Campus, Tiruchirappalli, Tamilnadu, India. His research interest is Fuzzy Graph Theory. He received M.Sc., M.phil., from Bharathidasan University, Tiruchirappalli, Tamilnadu. She did Ph.D from Gandhigram Rural University, Gandhigram. She did M.E. Computer Science from Anna University, Chennai. She has published 60 technical papers in International Journals.

Ramadevi P is working as Assistant Professor in Anna University – BIT Campus, Tiruchirappalli, Tamilnadu, India. His research interests are in the area of Cryptography and Network Security, VLSI Design, Embedded systems. She received the B.E. in Electronics and Communication Engineering from Bharathiyar University,Tamilnadu. M.Tech Software Engineering from Bharathidasan University, Tiruchirappalli, Tamilnadu. She is pursuing her Part time -PhD in Anna University Chennai.