DOI: https://doi.org/10.53555/nncse.v2i3.483 **Publication URL: http://nnpub.org/index.php/CSE/article/view/483**

DESIGN OF ENCRYPTION BLOCK FOR HIGH-SPEED LOW POWER BLOWFISH CIPHER

Sneha D. Meshram[1]*, U.M. Gokhale[2]
*[*12] Department of Electronics & Telecommunication Engg,GHRITW, Nagpur, India*
[1]**snehameshram.269@gmail.com*, [2]*umgokhale@gmail.com*

Corresponding Author: -
Email ID- *snehameshram.269@gmail.com*

Abstract: -

Data security always been important in all aspects of life. Data contain important information that must be protected from unauthorized access. As technology continues to dominance various operations in our day-to-day life so it is important. Reprogrammable devices are highly irresistible option for hardware execution of encryption algorithm. It is essential because these devices enhance cryptographic algorithm ability, physical security. Therefore, this paper scrutinizes the most important process in cryptographic algorithm i.e. Encryption. Here we used the Blowfish algorithm which is block cipher. All the basic blocks of this block cipher is designed by using VHDL.

Keywords: - *Algorithm block cipher Blowfish, cryptographic, encryption.*

I. INTRODUCTION

The internet is a universal system of linked computer networks that uses the standard Internet Protocol Suite (TCP/IP) to serve billions of planetary users. It is a network of networks which subsists of millions of private, public, academic, business and government networks of local to global range that are connected by a broad arrangement of electronic, wireless and optical networking technologies. With the rapid growth of internet, there is need to protect the sensitive data from unauthorized access. Whenever sensitive or privileged information is transmitted there is possibility of unauthorized third-party attack in order to learn the privileged information. This prospect is intolerable in many scenarios. For avoiding such type of scenario, we use cryptography.

Cryptography is the job of interpreting a message into a form which is unreadable to everyone except the purposive recipient. This is done with the help of key. In cryptography, keys are cast-off to encrypt a message into a format which would appear as unreadable random information to an unauthorized third party.

Originally DES (Data Encryption standard) based encryption strategy used in 1977 by FIPS (Federal Information Processing Standard). In DES data are encrypted in 64-bit block using 56 bits key. This strategy was considered as most sheltered strategy till 1998; because in 1998 EFF (Electronic Frontier Foundation) declared it developed DES cracker to crack code. After that AES (Advanced Encryption Standard) substituted DES in 2001 as the approved standard for a wide range of application. The structure of AES is complex and cannot be simply implemented. AES is a non-fiestel cipher that encrypt and decrypt a data block of 128 bits. The implementation of this AES algorithm utilizes more area. Solution on this problem is Blowfish cryptosystem.

The Blowfish cryptosystem, depicted by Bruce Schneier in 1993 to substitute DES (DATA ENCRYPTION STANDARD), even though it was introduced over a decade ago. If this system is accessible in hardware, such a system may be the most dominant tool for any communication system where high certainty is needed. This cryptosystem is designed and is implemented using VHDL language. It is used for high speed embedded applications such as mobile phone networks.Wireless communication schemes greatly require highly secured data encryption technique. In many of such application it is hard to cast-off software crypto approach. Therefore, hardware implementation of such type of system can be very useful for wireless application.

II. LITERATURE SURVEY

The concept of blowfish is very straightforward to understand but its true implementation and the use of algorithm in real time is very tangled. The paper is written by Author Brian Cody, Justin Madigan, Spencer MacDonald, Kenneth W. Hsu [5], provide the basic information about Blowfish algorithm The information states that Blowfish is a symmetric block cipher which can be used for encrypting and safeguarding of the data effectively. Blowfish has fixed 64-bit block size. Blowfish has a key which varies from 32 bits to 448 bits. Blowfish algorithm cipher is 16-round Fiestel network as well as it uses password dependent S-boxes. It subsists of complex initialization phase which is required before any encryption can take place. As blowfish block cipher which has variable key length, it is most acceptable for applications where the key does not often change like communication link or automatic file encryptor. The detailed concept of Fiestel network is described by Akshath . B.R, Amitabh K. Kumar, Neha Choubey, Jamuna S, Raja Jitendra Nayaka [3] which was published by Horst Fiestel in 1973. A Fiestel Network is said to be an iterative network composed of an internal function called as round function (also known as F-function) is altered into permutation. The working of Fiestel Network is summarized as follows: -

- The input data divide into two equal halves.
- The right half of input data become the new left half.
- The round function (F-function) act as a input to the right half of input data and the key.
- The resultant F-function is Xored with the left half of input data.
- The result obtained from the Xor operation is the new right half.
- The new right half and the new left becomes the Fiestel Network output.

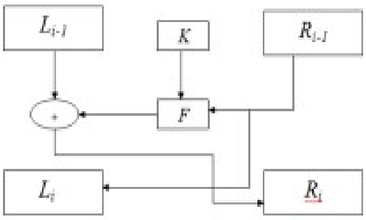

Figure 1: Fiestel Network

As indicated in introductory part Blowfish algorithm is a 64–bit block cipher. It has uneven key differing from 32 to 448 bits. This algorithm consists of two parts: Key expansion part and data encryption part. Key expansion part convert key which can be maximum of 448 bits into some sub key arrays of total 4168 bytes. The paper written by Mr. Tushar Joshi, Mr. Ravindra Yadav, Mr Utsav Malviya [1] elaborate the total blowfish algorithm in step wise manner with very efficient steps. They also propose the traditional way of hardware implementation as well as specify the particulars of S-boxes entries:

S1,0, S1, 1,..,S1,255;
S2,0, S2,,S2,255;

S3,0, S3,1,…,S3,255;
S4,0, S4,1,…,S4,255;

Data encryption part is occurred via 16 round Fiestel network. Each round consists of a key-dependent permutation, and a data dependent substitution. All operations are XORs and additions on 32-bit words. The only inclusional operations are four indexed array data look ups per round. It has following elements:

- P-array (Permutation boxes which perform shuffling or mixing)
- S-boxes (Substitution boxes, perform nonlinear function)
- XORing to obtain linear mixing.

These keys have to be precomputed before any data encryption or decryption. The key array also called P-array consist of 18 32-bit subkeys: P1, P2,..,P18.

A.Ramesh, Dr. A. Suruliandi[3] propose detailed performance analysis of various data encryption schemes like AES(Advanced Encryption Standard),DES(Data Encryption Standard) . This paper gives the comparative analysis between AES, DES, Blowfish algorithms in terms of security.

III. PROPOSED TECHNIQUE

The blowfish is a general-purpose algorithm. symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products.

The Main objective of Main proposed technique is to encrypt the data in very efficient manner.

There are three main operations performed in Blowfish algorithm. They are encryption, decryption and key generation. The encryption starts with the generation of F-function.

The diagram shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the Sboxes. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output.

Divide the left half i.e. XL into 4 bit quarter parts: a, b, c ,d. It is shown in figure 2

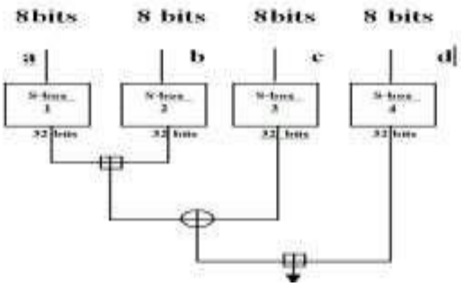

Figure 2: The Feistel Function of Blowfish

This Fiestel function plays an important role in key generation and encryption of the data. The generation of fiestel function can be shown with the help of flowchart.

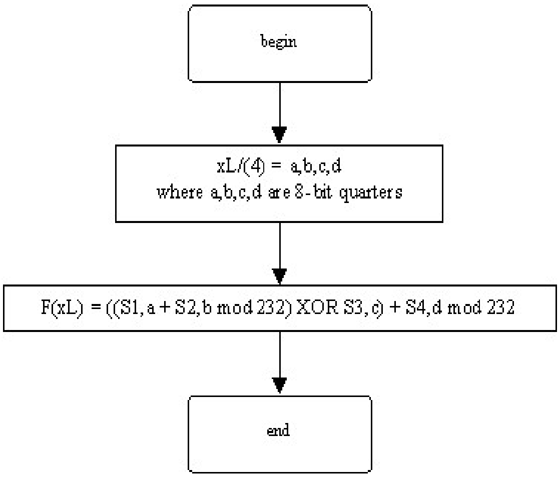
begin
xL/(4) = a,b,c,d
where a,b,c,d are 8-bit quarters
F(xL) = ((S1,a + S2,b mod 232) XOR S3, c) + S4,d mod 232
end

Figure 3: The Flowchart of Feistel Function Generation

RESEARCH METHODOLOGY

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.[2] It is a 16-round Feistel cipher and uses large key dependent In structure it resembles CAST-128, which uses fixed S-boxes.

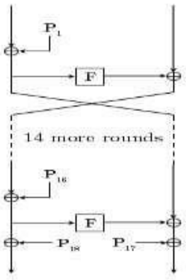

Figure 4: Encryption strategy of Blowfish

Each line represents 32 bits. The algorithm keeps two sub-key arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries. Blowfish performs 16 rounds of iteration. This algorithm can be shown with the help of flowchart.

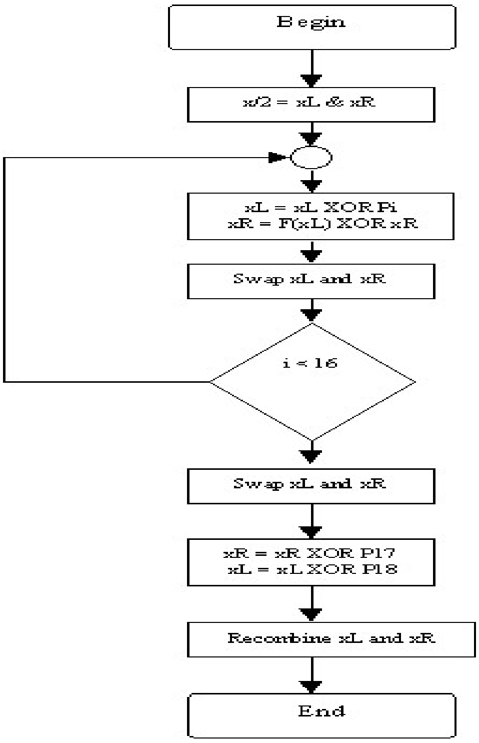

Figure 5: Flow of Encryption process

IV. RTL VIEWS AND SIMULATION RESULTS

The blowfish algorithm is designed by using some basic components. These components are designed in VHDL using Xilinx ISE 13.1. . First basic block is key dependent S-box. The RTL view is shown in figure 6.

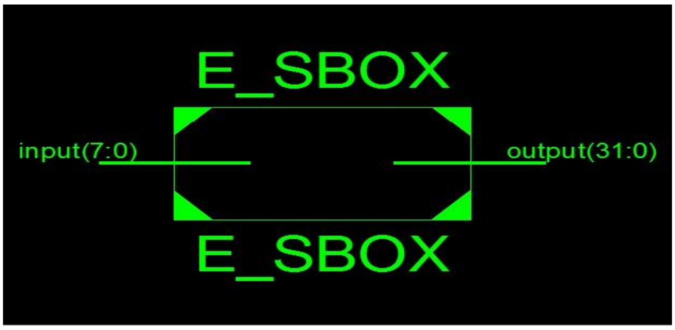

Figure 6. RTL view of S-box

Second block is fiestel network. Basically, fiestel network is a structure which makes encryption and decryption. The RTL view, simulation result is shown in figure 7 and 8 respectively.

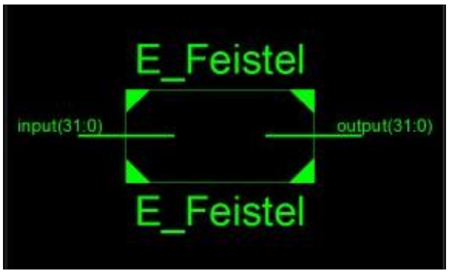

Figure 7 RTL view of Fiestel

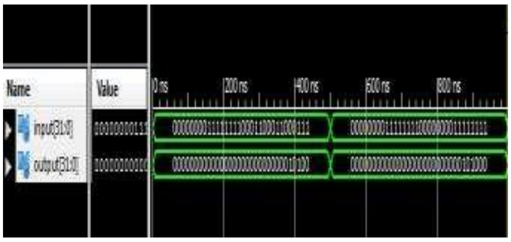

Figure 8 Simulation of Fiestel

Third most important block is encryption block. This block has two main key blocks i.e., S-box and Fiestel box. The working of this block is mainly depended on the 32-bit keys which has a total number 18. The RTL view, simulation result as shown in figure 9 and 10 respectively.

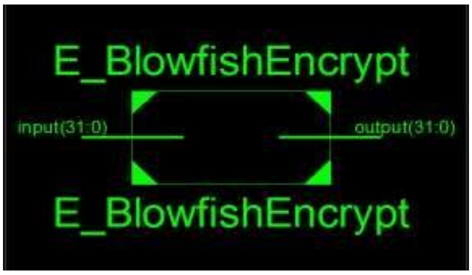

Figure 9 RTL view of Encryption block

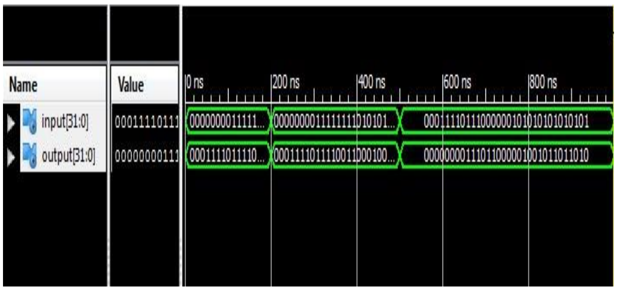

Figure 10 Simulation of Encryption Block

VI. CONCLUSION

If the key is strong in nature, then and only then the whole encryption block will be strong in nature. That means if keys are highly bounded with secrets, then the encryption process will generate highly bounded output. The resultant of this is that the blowfish algorithm will give most encrypted nature of data and the unauthorized access never steal the data.

REFERENCES

[1].Mr. Tushar Joshi Mr.Ravindra Yadav Mr. Utsav Malviya "Design Of Enhanced Speed Blowfish Algorithm For Cryptography With Merged Encryption & Decryption IN VHDL*", International Journal Of Engg Research And Applications* ISSN:2248-9622 April-2014 p.p. 68-71

[2].Ankita Deshpande P.S.Chaudhary "FPGAImplementation OF Blowfish CryptographicAlgorithm", *International Journal Of Advanced Research in Computer Scienceand Software Engineering,* ISSN:2277,*1*28X ,Volume 4,Issue 4, April-2014 p.p.

[3].A.Ramesh DR. A. Suruliandi" Performance Analysis OF Encryption Algorithms For Information Security", ",International Conference On Circuits, Power and Computing Technologies, IEEE 2013 p.p.840-844

[4].Akshatha.B.R Amitabh Kumar Neha Chobey Jamuna. S "FPGA Implementation OF Modified Blowfish Algorithm", International Conference On Electronics And Communication Eng Bengaluru, ISBN :978-93-83060-04-7 April-2013 p.p. 44-48

[5].Brian Cody Justin Madigan Spencer MacDonald, Kenneth W. Hsu "High Speed SOC Design For Blowfish Cryptographic Algorithm", IEEE 2007 p.p. 284- 287

[6].Cryptography & Network Security, William Stallings, Fifth Edition

[7].Jayaram. Bhasker, *A VHDL Primer*, 3rd edn , Prentice Hall publication, 2003.