TWOFISH ALGORITHM FOR ENCRYPTION AND DECRYPTION

*1 Anil G. Sawant,2 Dr. Vilas N. Nitnaware, 3Pranali Dengale, 4Sayali Garud, 5Akshay Gandewar
*1 Research Scholar (Asst. Professor) ,2 Principal, 3Student, 4Student, 5Student
*1 JJT University, Rajasthan, India (Trinity College of Engineering and Research, Pune), 2 D. Y. Patil School of Engineering Academy, Pune, India, 3Trinity College of Engineering and Research Pune, 4Trinity College of Engineering and Research, Pune5 Trinity College of Engineering and Research, Pune.
Email:* anilsawant.22@gmail.com, vilasan30@yahoo.com, pranalidengale@gmail.com, sayaligarud1997@gmail.com, akkigandewar@gmail.com

Abstract **-** In this paper, a novel VLSI architecture of the TWOFISH block cipher is presented. TWOFISH is one of the most secure cryptographic algorithm. The characteristic features of the TWOFISH Algorithm are good security margin and has fast encryption/decryption in software, moderately fast in hardware and moderate flexibility. Based on the loop-folding technique combined with efficient hardware mapping, the architecture of twofish Algorithm can make data encryption/ decryption more efficient and secure. To demonstrate the correctness of our Algorithm , a prototype chip for the architecture has been implemented. The chip can achieve an encryption rate and low power consumption while operating clock rate. Designed TWOFISH cryptographic algorithm improved the MDS block that improved a process speed, and decreased complexity and power consumption. Therefore, the chip can be applied to encryption in high-speed networking protocols like ATM networks. This paper will be implemented in Xilinx 14.2 in Verilog HDL.

Keywords - Verilog , MDS, PHT, DES, Function F and h.

I. INTRODUCTION

Cryptography is the process for combining the plain-text and a user-specified key to generate an encrypted output which is called the cipher-text. In cryptographic security it is required that if the cipher-text is given, nobody is able to recover the original plaintext without the key[1][4] .There are two kinds of cryptographic algorithms: symmetric and asymmetric. In symmetric algorithms, similar key (the secret key) is used to encrypt and decrypt the data/message, and in asymmetric algorithms one key (called as public key) is used to encrypt the message and a different key (called as private key) to decrypt it [2][4].Symmetric key algorithms can be divided into two categories, stream ciphers and block ciphers. Stream ciphers encrypt the single bit of plaintext at a time; whereas block ciphers operate on the plaintext in group of bits, called blocks. TWOFISH is a 128-bit block cipher algorithm and can work with the keys of variable-lengths[3]. There is a 16-round Feistel network with a function F made up of four key-dependent 8-by-8-bit S-boxes [1], a fixed 4-by-4 maximum distance separable (MDS), a pseudo-Hadamard transform (PHT).

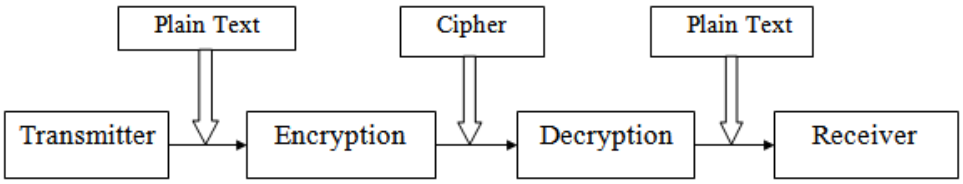

Fig 1-Block Diagram

II.TWOFISH Algorithm

TWOFISH is a 128-bit block cipher algorithm that accepts a variable-length key[1][2][3]. The cipher is a 16-round network with a bijective F function made up of four key- dependent 8-by-8-bit S-boxes, a fixed 4-by-4 maximum distance separable matrix. In twofish algorithm, the input and output data are XOR-ed with eight sub-keys K0…K7. These X-OR operations are called input and output whitening[1]. The F-function consists of five kinds of component operations: key dependent S-boxes, Maximum Distance Separable (MDS) matrices, Pseudo-Hadamard Transform (PHT).

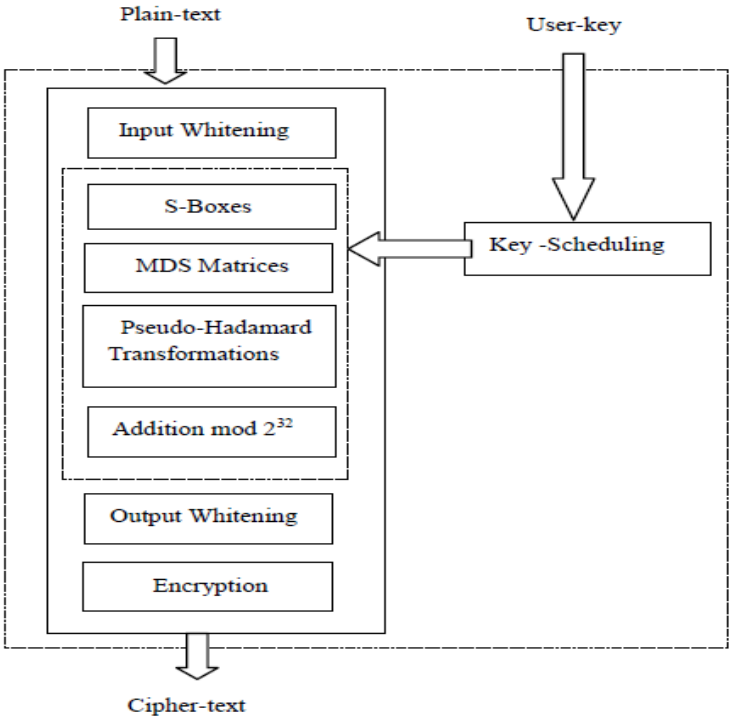

Fig 2 - TWOFISH Algorithm steps

In twofish algorithm, the input and output data are XOR-ed with eight sub-keys K0…K7. These X-OR operations are called input and output whitening. There are four kinds of key dependent S-boxes combine with the MDS matrix form and g-function. There are total 16-rounds in the twofish algorithm[2]. Some building blocks of twofish algorithms are:

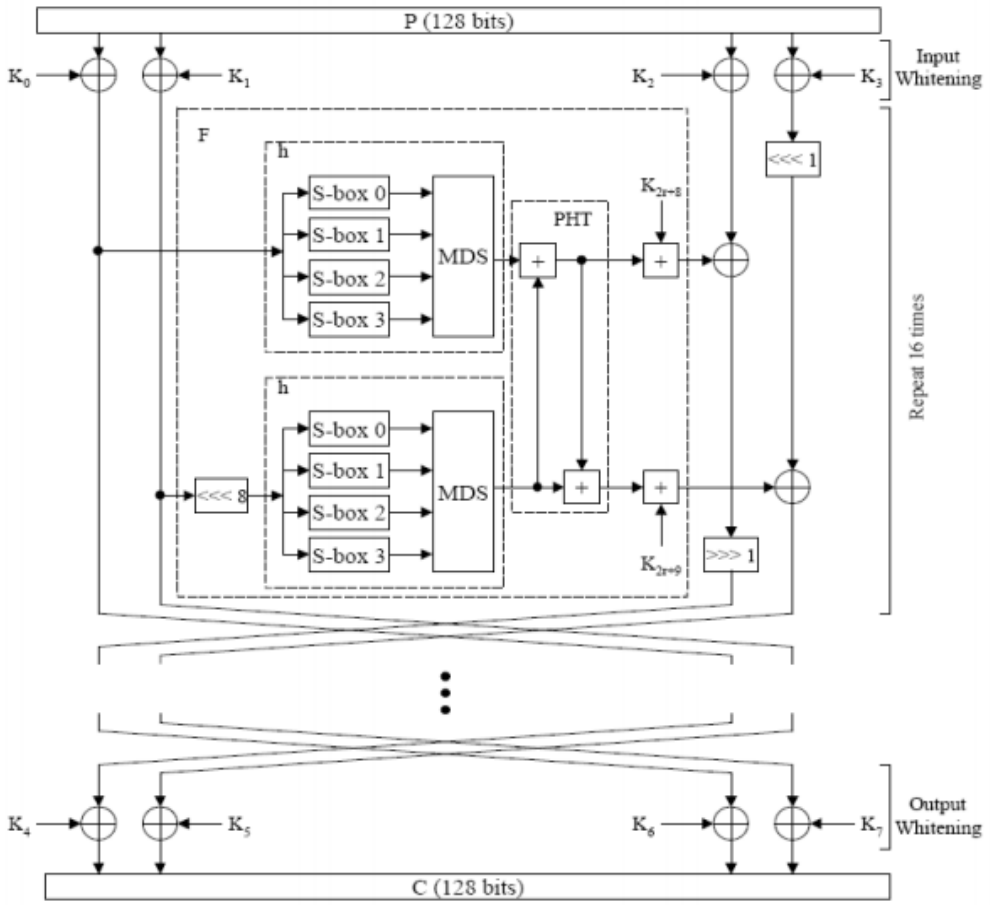

Fig 3-TWOFISH Structure

S-Box-

S-box is An a table- driven substitution operation used in many algorithms. It can change in both input and output size and can be made randomly or algorithmically[3]. There are four kinds of s-boxes used in the twofish algorithm. The four different S-boxes together with the MDS matrix form an h-function. This h-function appear two times in the algorithm which causes significant

redundancy. In Twofish, each S-box consist of three 8-by-8-bit fixed permutations chosen from a set of two possible permutation, q0 and q1. The XOR operation are performed with two sub-keys.

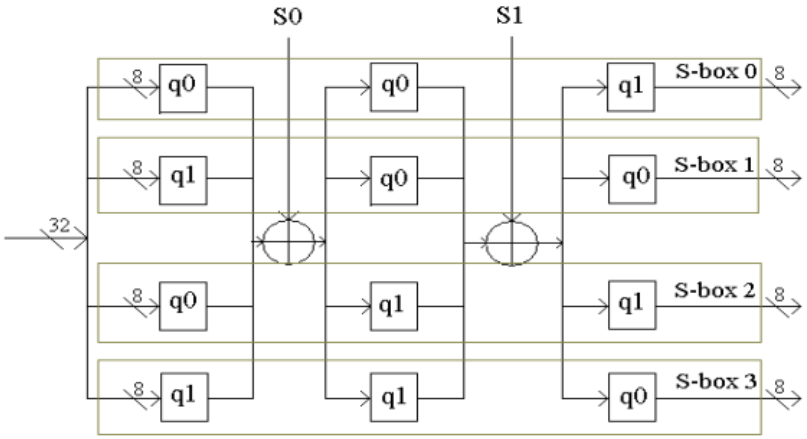

Fig 4- Architecture of S box

MDS Matrix-

The twofish algorithm uses a single 4-by-4 Maximum Distance Separable (MDS) matrix[1][2]. The MDS Matrix is used as the main diffusion mechanism for the four bytes output by the four S-boxes. MDS matrices are useful building block for ciphers because they guarantee a certain degree of diffusion. If one of the input element is changed, all the output element must change. If two input element are changed, all but one of the output element must change.

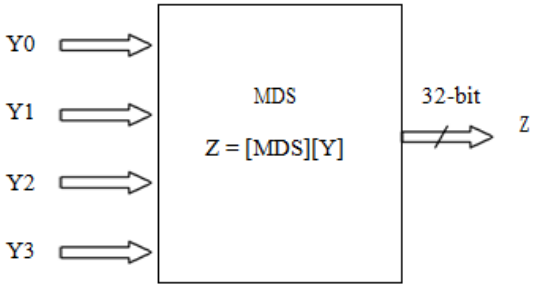

Fig 5-MDS

Pseudo-Hadamard Transforms (PHT)-

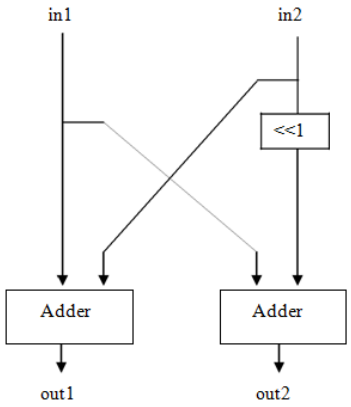

Fig 6-Architecture of PHT

A pseudo-Hadamard Transform (PHT) is a simple mixing operation that is very efficient in the software[3]. To optimize the performance of the Twofish a version of the code used for encryption and decryption. Twofish uses a 32-bit PHT to mix the output from its two parallel 32-bit h -function.

F Function-

The Twofish block cipher is a 16-round Feistel-like network. It is a not cost effective to map directly the 16-round encryption operation into hardware. Thus we fold the 16-rounds loop operations into one-round operation. The one-round operation is performed by the F-function Unit.

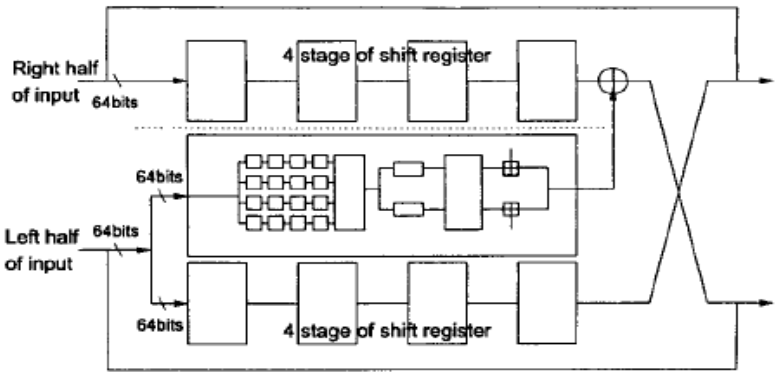

Fig 7-Architecture of F function

H Function-

The function h forms the heart of twofish. Each S-box takes 8 bits of input, and produces 8 bits of output as shown in Fig8. The four results are interpreted as a vector of length 4 over GF(28), and multiplied by the 4x4 MDS The resulting vector is interpreted as a 32-bit word which is the result of h.

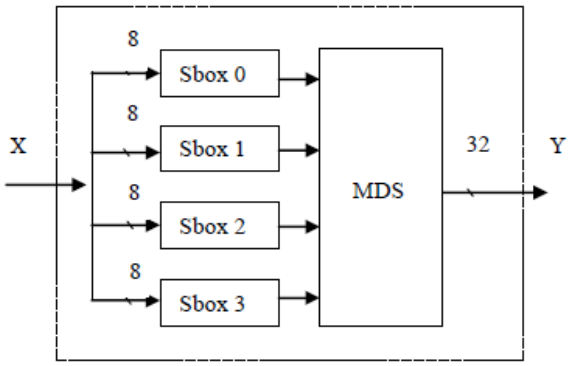

Fig 8-Architecture of H function

Future Work –

Twofish, has been verified by functional simulation, using Xilinx 14.2, and Model-Sim Simulator for the waveform generation. The modules MDS and PHT had been modified and implemented for the modified algorithms. All the modules and functions are interrelated hence, after modifying MDS and PHT function g and function F also got modified. The results show the delay of twofish algorithm of 128-bit key and modified twofish of 128-bit key, we compared their delay results. The analysis shows that modified algorithm has less delay then the conventional one. After that the delay results of twofish algorithm with 192-bit key and modified twofish with 192-bit key have been compared. According to the results it is clear that modified 192-bit key twofish algorithm has less delay than 192-bit twofish. In future, it is intended to implement the algorithm on sensor networks and ad-hoc networks on cross-layer. Also, the other modules of algorithm can be modified to reduce further delay.

Conclusion-

The information security can be easily achieved by using Cryptography technique. A large number of encryption algorithm have been developed to secure our confidential data from the hackers. But some algorithm 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. Our information can be secured if it is encrypted by using multiple keys or a large bit stream of key (i.e. 128-bit,256-bit,etc.). But to achieve this is a large computational time is required, giving a large delay which can be harmful to us. The hacker can hack the information during this time. The use of FPGAs can help us to improve this limitation because FPGAs can give enhanced seed. This is due to fact that the hardware implementation of most encryption algorithm can be done on FPGA.

References-

[1] Bruce Schneier, John Kelsey, Doug Whitingz David Wagnerx Chris Hall, Niels Ferguson “Twofish: A 128-Bit Block Cipher” AES submission, 1998.
[2] Shun-Lung Su, Lih-Chyau Wuu, and Jhih-Wei Jhang, “A New 256-bits Block Cipher –Twofish 256”, Computer Engineering & Systems, International Conference in IEEE, 2010, pg 166 - 171
[3] Mark De Clercq, Vincent Levesque “A VHDL Implementation of the Twofish Block Cipher” in IEEE, 2006.
[4] Hani H. JABER “Relational Database Security Enhancements”, in Arab University, 2008.