UACEE International Journal of Advances in Electronics Engineering – IJAEE
Volume 3 : Issue 2 [ISSN 2278 – 215X]
Publication Date : 05 June 2013

Twofish Algorithm and its Implementation on FPGA

[Purnima Gehlot, Richa Sharma, S. R. Biradar]

***Abstract* — Now-a-days internet is one of the most important source of communication and thousands of people interact electronically. For sending sensitive messages over the internet, we need security. In this paper a security algorithm, Twofish has been explained with all of its modules with both 128 and 192-bit key size. Implementation on Xilinx – 6.1 xst software has been done taking delay as main constraint.**

***Keywords*—twofish, MDS, PHT, symmetric key, Function F and g.**

I. Introduction

Twofish is a 128-bit block cipher and can work with the keys of variable-lengths up to 256 bits. There is a 16-round Feistel network with a function F made up of four key-dependent 8-by-8-bit S-boxes [3], a fixed 4-by-4 maximum distance separable (MDS) matrix over GF(2^8), a pseudo-Hadamard transform (PHT), [1] bitwise rotations, and a carefully designed key schedule. In twofish algorithm, same key used for both the encryption and decryption purpose that's why it is called as symmetric key algorithm.

II. Aim of Paper

Objective of this paper is to perform an efficient method of implementing a twofish algorithm with minimum delay and having high performance in terms of power and area used while maintaining the proper functionality of the system. The software used for the implementation of the algorithm is Xilinx 6.1 – xst and language used is VHDL (very high speed integrated circuit hardware description language). Simulation of encryption process of the twofish algorithm has been done using the Xilinx software. Inputs will be converted into binary form and given as input to the "Model-Sim Simulator" of Xilinx 6.1 xst, and in the output we will get the RTL diagram, the waveform and the synthesis report, from which we will get the values of delay, area and power. Here two simulations for PHT i.e. pseudo hadamard transform has been performed. Structure of Twofish algorithm is shown in Figure 1.

The organisation of paper is like this, First of all the description of all the modules of algorithms with appropriate diagram has been given, then the results after their simulation and then output waveforms.

Purnima Gehlot, Richa Sharma (Student)
MITS University
India
purnima.gehlot20@gmail.com, Sharma.r0707@gmail.com

S. R. Biaradar (Professor)
MITS University
India
srbiradar@gmail.com

III. Research Objective/Question

To reduce the delay of network security algorithm so that it can provide best network security with minimum delay, and to find out why Twofish algorithm is rarely used though it has better security factor than commonly used security algorithm. We will try to reduce the delay in Twofish algorithm.

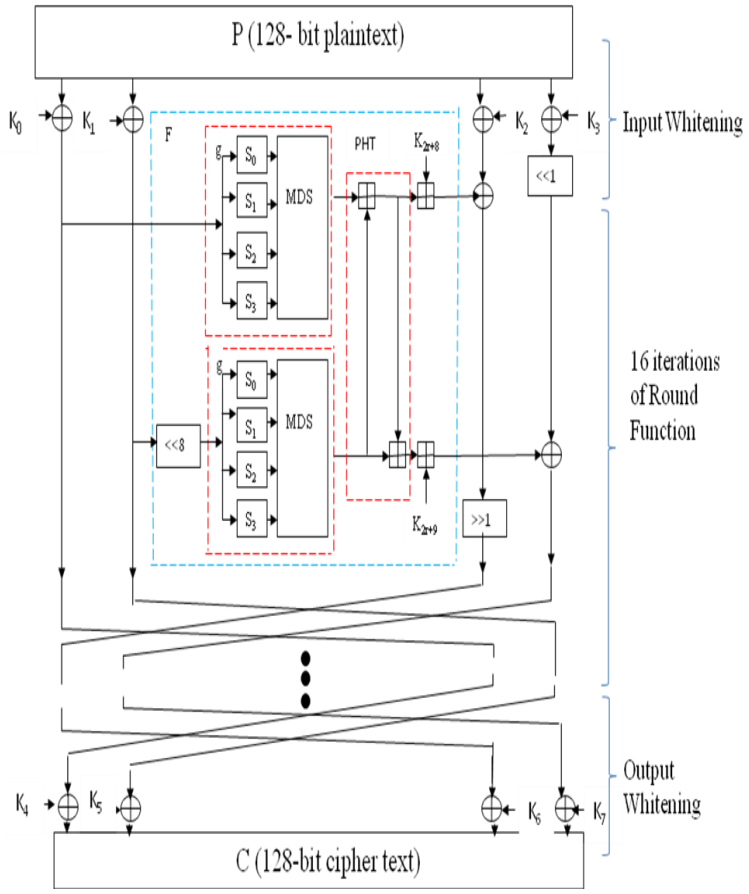

Figure 1. Twofish Structure

IV. Modules of Twofish Algorithm

Mainly there are three main steps in this algorithm, input whitening, sixteen iterations of round function and output whitening. [4] Input is combined mathematically with the keys (key is divided into bytes and XORed with the input bytes). This process was input whitening. After 16 rounds same process happens in output whitening. During the rounds, function F is the main module for it, which consists other modules which are function g, MDS i.e. maximum distance separable matrix, PHT i.e. pseudo hadamard transform and two adders of 32-bit for one round. To increase the complexity

of the algorithm we can perform Endian function over the input bit stream. Different modules of twofish algorithms are:

A. *Endian Function*

Endian Function is a transformation of the input data. It is used as an interface between the input data provided to the circuit and the rest of the cipher. It can be used with all the key-sizes [6].

The function of Endian block can be explained easily with the help of Figure 2. Here 128-bit input is divided into 16 bytes from byte0 to byte15 and are rearranged to get the output of 128-bit. Simulation result is shown in Table I.

B. *PHT (Pseudo Hadamard Transform)*

PHT is a reversible transformation of a bit string that provides cryptographic diffusion. SAFER was the first cipher block which uses 8-bit PHTs extensively for diffusion [5]. Twofish uses a 32-bit PHT. The outputs from the two g functions are given as input to the PHT module, it performs some addition operations over it and produces output. It is a two input, two output function.

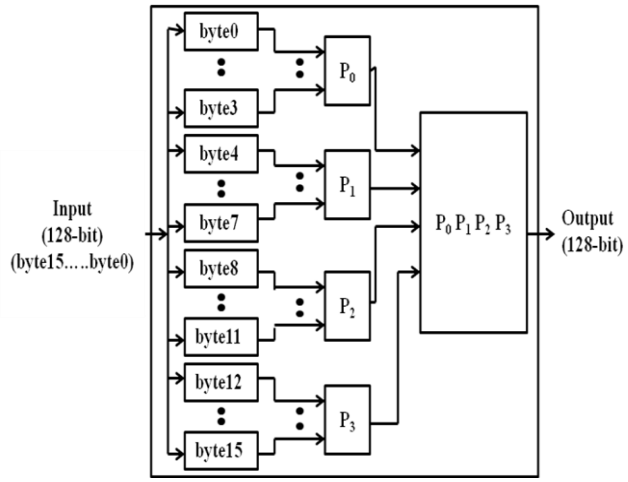

Figure 2. Endian Function

Given two inputs, a and b, the 32-bit PHT is

$a' = a + b \bmod 2^{32}$

$b' = a + 2b \bmod 2^{32}$

The method to implement the PHT module is explained below.

Direct addition is performed for both the outputs using 32-bit adder block as shown in Figure 3.

For first Output

C = A+B

Output1 = C

For second Output

Output2 = C + B

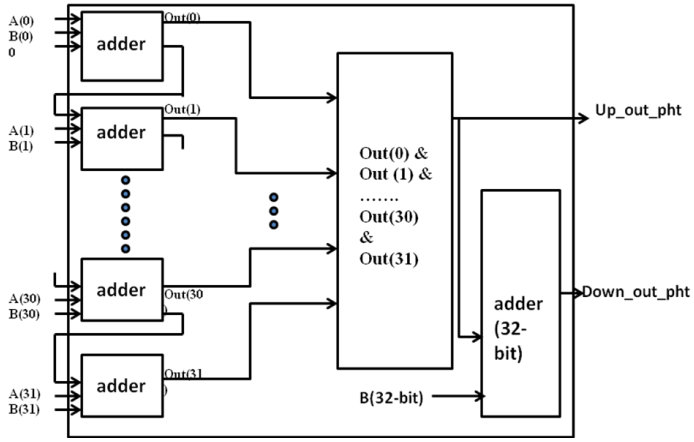

Figure 3. PHT

C. *MDS (Maximum Distance Separable) Matrix*

A 4-by-4 MDS matrix is used in twofish algorithm. MDS matrices are useful building blocks for ciphers [3] because they guarantee a certain degree of diffusion. MDS matrix is shown in Figure 4. There are only three coefficients in MDS matrix, 01, EF and 5B [2]. The result of a multiplication can be reduced to a series of XOR's for each bit of the output.

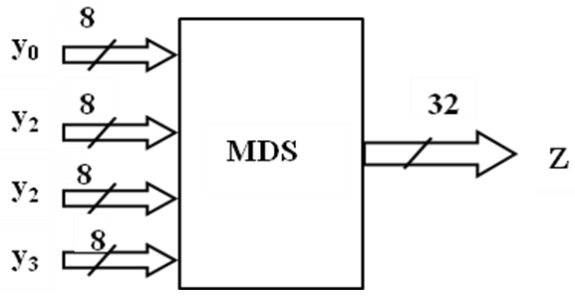

Figure 4. MDS Structure

Figure 4. shows the basis function in MDS block of twofish algorithm.

y0_ef = y0 * ef (1)

y0_5b = y0 * 5b (2)

y1_ef = y1 * ef (3)

y1_5b = y1 * 5b (4)

y2_ef = y2 * ef (5)

y2_5b = y2 * 5b (6)

y3_ef = y3 * ef (7)

y3_5b = y3 * 5b (9)

using above equations we can determine

z0 = y0 ^ y1_ef ^ y2_5b ^ y3_5b (11)

z1 = y0_5b ^ y1_ef ^ y2_ef ^ y3 (12)

z2 = y0_ef ^ y1_5b ^ y2 ^ y3_ef (13)

z3 = y0_ef ^ y1 ^ y2_ef ^ y3_5b (14)

using above four equations we get

Z = z3 & z2 & z1 & z0

Z = [MDS] [Y]

$$\begin{pmatrix} z0 \\ z1 \\ z2 \\ z3 \end{pmatrix} = \begin{pmatrix} 01\ EF\ 5B\ 5B \\ 5B\ EF\ EF\ 01 \\ EF\ 5B\ 01\ EF \\ EF\ 01\ EF\ 5B \end{pmatrix} \begin{pmatrix} y0 \\ y1 \\ y2 \\ y3 \end{pmatrix}$$

D. *Function g*

It consists of two main elements, the key-dependent S-boxes and the MDS matrix. 32-bit input is divided into 4-bytes. The internal structure for this function is shown in Figure 5. below.

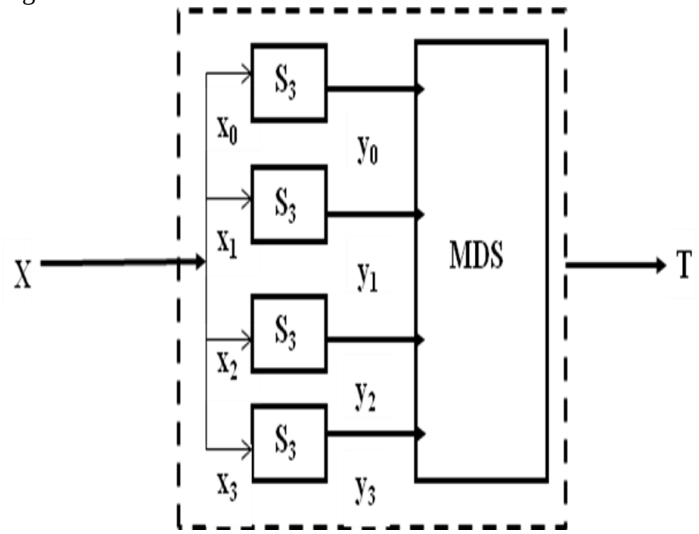

Figure 5. Function g

E. *Function F*

Function F is the main operation of the algorithm. It consists of four key-dependent 8-by-8-bit S-boxes, a fixed 4-by-4 maximum distance separable matrix, a pseudo-Hadamard transform [5], bitwise rotations and a key schedule as shown in Figure 6. The operations of this function can be explained easily by:

$T_0 = g(R_0)$
$T_1 = g(ROL(R_1, 8))$
$F_0 = (T_0 + T_1 + K_{2r+8}) \bmod 32$
$F_1 = (T_0 + 2T_1 + K_{2r+9}) \bmod 32$

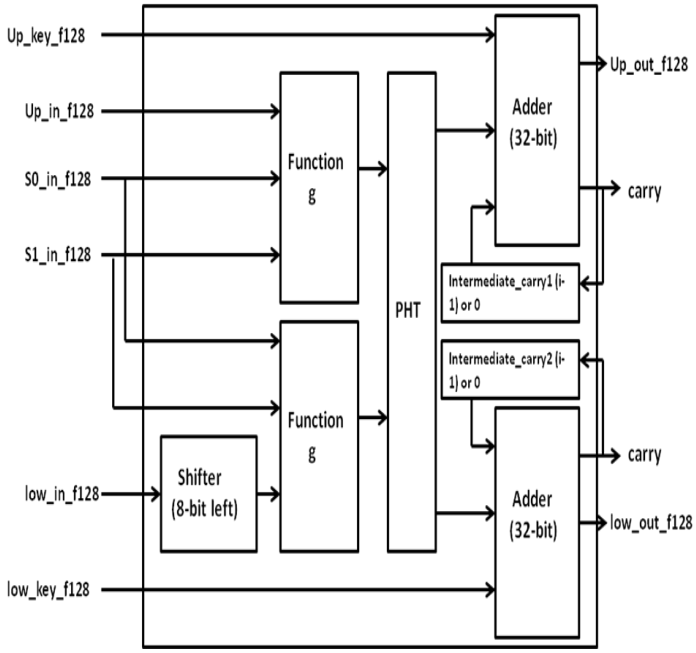

Figure 6. Function F

F. *Encryption*

Encryption is the process of converting the data from plain-text to cipher. Here in this paper encryption of 128-bit input is considered for one round. The output of encryption will be given for output whitening and we will get the cipher-text as output.

V. Work and Findings so far

Table I. and Table II. shows the delays of all the modules and delay for encryption along with the frequency in MHz for 128-bit key size and 192-bit key size respectively.

Table I. Delay and Frequency of Different Modules for 128-bit key size

Parameters	Delay (ns)	Frequency (MHz)
Endian	6.479	154.34
Function F	104.102	9.60
Function g	39.383	25.39
MDS	15.520	62.81
PHT	61.172	16.34
Encryption	105.794	9.40

Table II. Delay and Frequency of Different Modules for 192-bit key size

Parameters	Delay (ns)	Frequency (MHz)
Endian	6.479	154.34
Function F	113.822	8.78
Function g	49.076	20.37
MDS	15.524	64.41
PHT	67.850	14.73
Encryption	115.307	8.67

VI. Future Work

Our aim is to implement the algorithm with lowest possible delay and which provides the best network security and its application in providing sensor network security where area is the main concern.

Ms. Purnima Gehlot has completed her B.E. from MIT, Ujjain (M.P.) in Electronics and Communication Engineering and pursuing M.Tech in VLSI Design from MITS, Laxmangarh, India. Her research interest includes network security and privacy.

Ms. Richa Sharma has completed her B.Tech from RCEW, Jaipur (Raj.) in Electronics and Communication Engineering and pursuing M.Tech in VLSI Design from MITS, Laxmangarh, India. Her research interest includes network security and privacy.

Mr. S.R. Biradar is a Professor in the department of CSE, MITS, Lakshmangarh, India. He received his B.E, M.Tech and Ph.D degrees in Computer Science and Engineering from Karnataka University, MAHE Manipal and Jadavpur University respectively. His research interest includes Mobile Ad-hoc networking, advanced wireless communication.

VII. References

[1] Dr. S.A.M Rizvi, Dr. Syed Zeeshan Hussain, Neeta Wadhwa, "Performance Analysis of AES and TwoFish Encryption Schemes" in *International Conference on Communication Systems and Network Technologies of IEEE Computer Society*, 2011, pg. 76-79, vol-3

[2] Bruce Schneier, John Kelsey, Doug Whitingz David Wagnerx Chris Hall, Niels Ferguson "Twofish: A 128-Bit Block Cipher" *AES submission*, 1998.

[3] 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

[4] Mark De Clercq, Vincent Levesque "A VHDL Implementation of the Twofish Block Cipher" in *IEEE*, 2006

[5] Hani H. JABER "Relational Database Security Enhancements", in *Arab University*, 2008

[6] Uskov, A.V, "Information Security of IPsec-based Mobile VPN: Authentication and Encryption Algorithms Performance" Trust Security and Privacy in Computing and Communication, 11th International National Conference *in IEEE*, 2012, pg. 1042-1048