Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL

Purnima Gehlot
MITS University,
Laxmangarh (Raj.)

S. R Biradar
MITS University,
Laxmangarh (Raj.)

B. P. Singh
MITS University,
Laxmangarh (Raj.)

ABSTRACT
Now-a-days internet is one of the most important sources of communication and thousands of people interact electronically. For sending sensitive messages over the internet, we need security. Hence for secure communication required the algorithms. Among these algorithms is Twofish, a promising 128-bit block cipher and one of the competitors in National Institute of Standards and Technology's (NIST) AES competition, for the replacement of DES at the core of many encryption systems world-wide. In this paper the security algorithm, twofish has been explained with all of its modules (some modules has been modified) for both 128 and 192-bit key size. Implementation on VHDL using Xilinx – 6.1 xst software has been done taking delay as main constraint.

General Terms
Algorithms, Security, symmetric key, path delay

Keywords
Twofish, MDS, PHT, DES, Function F and g

1. INTRODUCTION
Cryptography is the process of 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. The algorithms which are used to fulfill the purpose are called as ciphers. The science of breaking ciphers, i.e. retrieving the plaintext from the cipher-text without knowing the proper key is called as cryptanalysis [4]. The branch of mathematics encompassing both cryptography and cryptanalysis is called cryptology. There are two kinds of cryptographic algorithms: symmetric and asymmetric. In symmetric algorithms, same 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 a message and a different key (called as private key) to decrypt it. Symmetric key algorithms can be divided into two categories, stream ciphers and block ciphers. Stream ciphers encrypt a single bit of plaintext at a time; whereas block ciphers operate on the plaintext in group of bits, called blocks. Most of the block ciphers are composed of usually 8 to 32 iteration rounds, where each iteration contains nonlinear substitution boxes (S-Boxes) followed by linear permutations. Block ciphers are flexible in nature; they can be used to design stream ciphers. Because of this flexibility, they are the workhorse of modern cryptography. Twofish is a 128-bit block cipher and can work with the keys of variable-lengths. 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) matrix over GF(2^8), a pseudo-Hadamard transform (PHT), bitwise rotations, and a carefully designed key schedule. In twofish algorithm, same key used for both encryption and decryption purpose that's why it is called as symmetric key algorithm. Twofish is a Feistel cipher, which are given by Horst Feistel in 1973, which are also called DES-like ciphers, are a special class of iterated SPN ciphers where the cipher-text is calculated from the plaintext by repeated application of the same transformation or round function [2]. Furthermore, in a Feistel cipher, the cipher-text being encrypted is split into two halves. The main advantage of Feistel network is that encryption and decryption is almost similar.

2. AIM OF THE 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 modified 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 and area.

The organization of paper is like this, First of all the introduction to cryptography and then twofish algorithm has been given then the basic algorithm has been explained. Then the description of all the modules of algorithms with appropriate diagram has been given under the heading 'twofish functions and modules', then the results of modified encryption and decryption on both 128 and 192-bit key are given in Table 1 and 2 and there comparison on the basis of delay.

3. TWOFISH ALGORITHM
Twofish is a 128-bit block cipher that accepts a variable-length key. The cipher is a 16-round Feistel 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 over GF(28), a pseudo-Hadamard transform, bitwise rotations, and a carefully designed key schedule. Twofish can be easily explained with the diagram as shown in Fig 1, 128-bit plain-text (divided into four parts of 32-bit each) is given for the input whitening where it is XOR-ed with four keys then function g PHT which are explained under the heading twofish functions and modules. Twofish can be implemented in hardware in 14000 gates [3]. The design of both the round function and the key schedule permits a wide variety of tradeoffs between speed, software size, key setup time, gate count, and memory. Twofish has been extensively cryptanalyzed and even the best attack is able to break only five rounds of the algorithm.

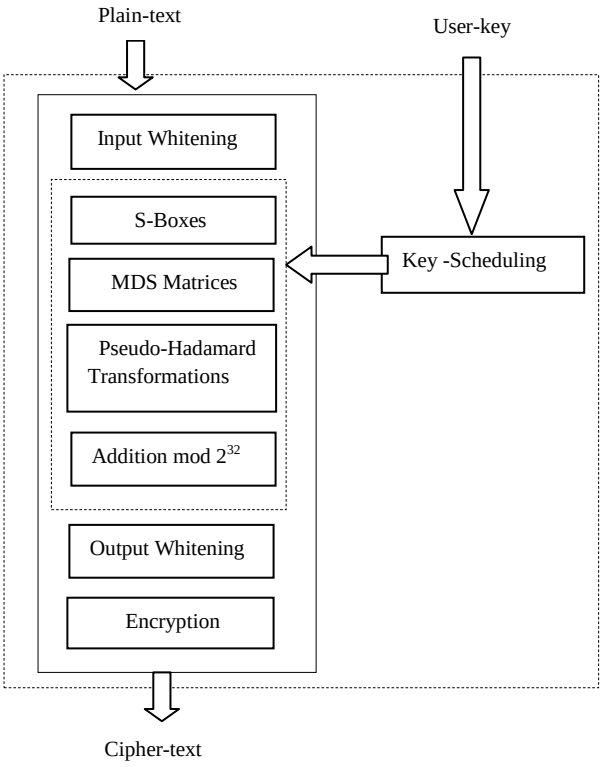

Fig 1: Twofish Algorithm steps

In twofish algorithm, input and output data are XOR-ed with eight sub-keys K0…K7. These XOR operations are called input and output whitening. The F-function consists of five kinds of component operations: fixed left rotation by 8 bits, key dependent S-boxes, Maximum Distance Separable (MDS) matrices, Pseudo-Hadamard Transform (PHT), and two sub-key additions modulo 2^{32} as shown in Fig 2. There are four kinds of key dependent S-boxes together with the MDS matrix form and g-function. This g-function appears two times in the cipher structure, which causes significant redundancy. There are total 16-rounds in twofish algorithm. Some building blocks of twofish algorithms are:

3.1 S-Box

Key dependent S-boxes are something new in a cipher design. In majority of known ciphers, S-boxes are used as a non-linear fixed substitution operation. In twofish, each S-box consists of three 8-by-8-bit fixed permutations for 128-bit and four for 192-bit, chosen from a set of two possible permutations, q0 and q1 [6]. Between these permutations, XOR operations are performed with sub-keys S0, S1 for 128-bit and there are three keys S0, S1 and S2 for 192-bit. The internal block diagram of s-boxes for 128-bit and 192-bit are shown in Fig 3 and 4 respectively. A 32-bit data is divided into four bytes which are alternatively given to q0 and q1 and then combined with sub-keys as shown in figure. These sub-keys are computed only once for a particular global key, and stay fixed during the entire encryption and decryption process.

$b_4 = t_3 [b_3]$

$y = 16b_4 + a_4$ (3.1)

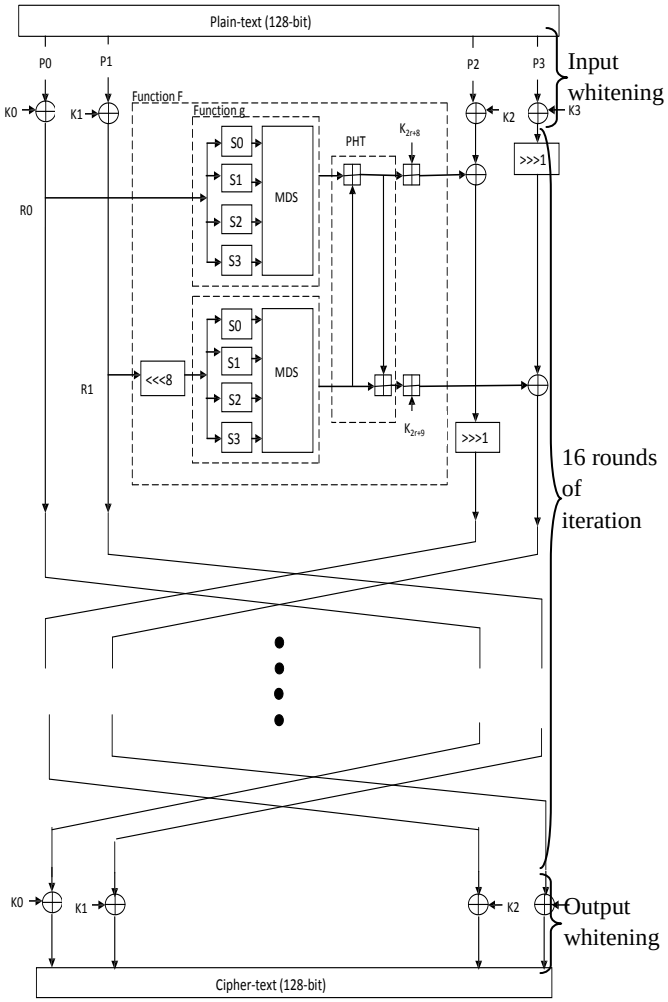

Fig 2: Twofish Structure

3.2 Q-Permutation

The Q-Permutation is at the core of the design of twofish. The permutations q0 and q1 are fixed permutations on 8-bit values. These permutation functions are the main components of the S-boxes [8]. They are constructed from four different 4-bit permutations each as shown in Fig 5. For the 8-bit input value x, the corresponding output value y is found by the following steps:

$a_0 = [x / 16]$ and $b_0 = x \bmod 16$

i.e., the byte is first split into two 4-bit nibbles, a0 and b0

$a_1 = a_0 \oplus b_0$

$b_1 = a_0 \oplus \text{ROR}(b_0, 1) \oplus (8a_0 \bmod 16)$

$a_2 = t_0 [a_1]$

$b_2 = t_1 [b_1]$

$a3 = a2 \oplus b2$

$b3 = a2 \oplus \text{ROR}(b2, 1) \oplus (8a2 \bmod 16)$

$a4 = t2 [a3]$

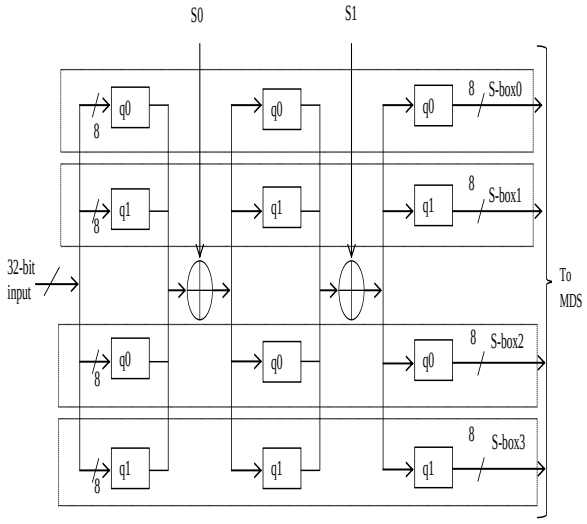

Fig 3: Internal Structure of S-box for 128-bit key

As in equation (3.1), these nibbles are combined in a bijective mixing step. Each nibble is then passed through its own 4-bit table look-up [7]. This is followed by another mixing step and table lookup. Finally, the two nibbles are recombined into a byte. The equation set (3.1) describes both of the permutations q0 and q1, but the lookup tables t0,…,t3 are different for q0 and q1. For the permutation q0, lookup tables are given by:

t0 = [8 1 7 D 6 F 3 2 0 B 5 9 E C A 4]
t1 = [E C B 8 1 2 3 5 F 4 A 6 7 0 9 D]
t2 = [B A 5 E 6 D 9 0 C 8 F 3 2 4 7 1]
t3 = [D 7 F 4 1 2 6 E 9 B 3 0 8 5 C A]

where each lookup table is represented by a list of the entries using hexadecimal notation. (The entries for the inputs 0,1,…,15 are listed in order.) Similarly, for q1 the lookup tables are given by:

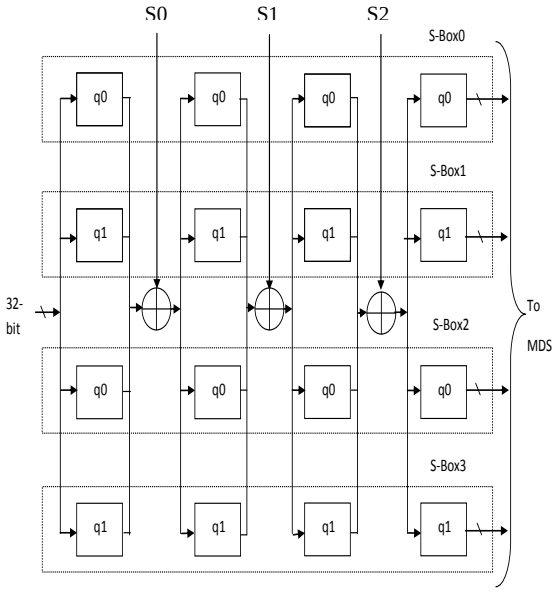

Fig 4: Internal Structure of S-box for 192-bit key

t0 = [2 8 B D F 7 6 E 3 1 9 4 0 A C 5]
t1 = [1 E 2 B 4 C 3 7 6 D A 5 F 9 0 8]
t2 = [4 C 7 5 1 6 9 A 0 E D 8 2 B 3 F]
t3 = [B 9 5 1 C 3 D E 6 4 7 F 2 0 8 A]

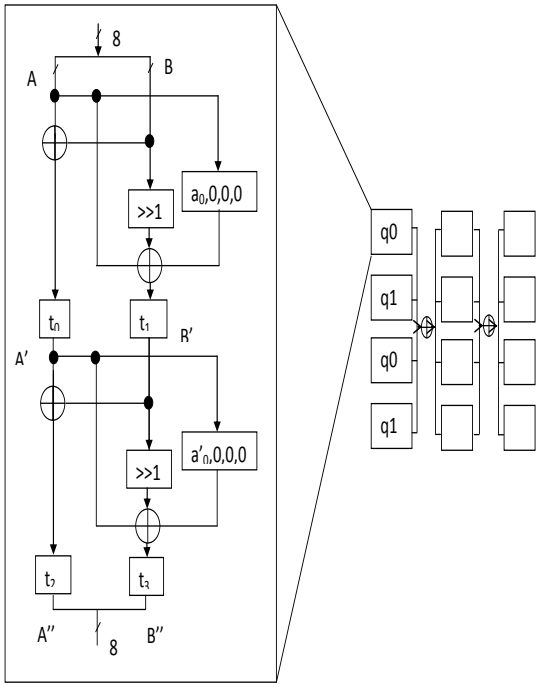

Fig 5: Internal Structure of q0

4. TWOFISH FUNCTIONS AND MODULES

4.1 Function F

The Feistel function F is a key-dependent permutation on 64 bit values. It takes three arguments, two input words P0 and P1, and the round number r used to select the appropriate sub keys. R0 is passed through the g function, which yields T0. R1 is rotated left by 8 bits and then passed through the g function to yield T1 [9]. The results T0 and T1 are then combined in a PHT and two words of the expanded key are added. The following set of equations describes the details of F function:

T0 = g(R0)
T1 = g(ROL(R1; 8))
F0 = (T0 + T1 + K_{2r+8}) mod 2^{32}
F1 = (T0 + 2T1 + K_{2r+9}) mod 2^{32}

4.2 Function g

The function g forms the heart of twofish. The input word X is split into four bytes. Each byte is run through its own key-dependent S-box. Each S-box is bijective, takes 8 bits of input, and produces 8 bits of output as shown in Fig 6. The four results are interpreted as a vector of length 4 over GF(2^8), and multiplied by the 4x4 MDS matrix (using the field GF(2^8) for the computations). The resulting vector is interpreted as a 32-bit word which is the result of g.

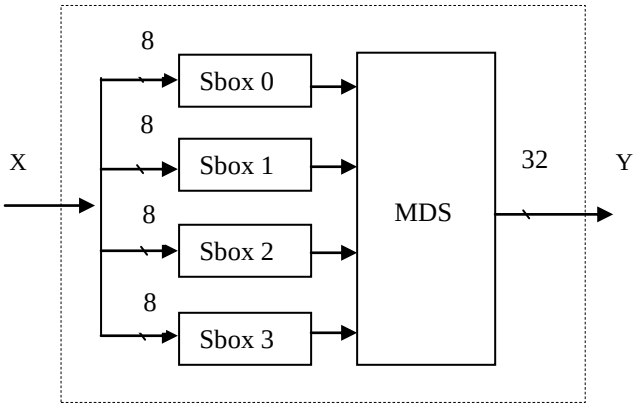

Fig 6: Function g

4.3 MDS

MDS is maximum separable matrix. It is a matrix of bytes that multiplies a vector of four bytes. Multiplications are carried out in the Galois Field GF(2^8) with the primitive polynomial $x^8 + x^6 + x^5 + x^3 + 1$. Each byte is converted into a polynomial in which each power p of x is present only if the p-th bit is 1. A multiplication in GF amounts to a multiplication of polynomials followed by a division by the primitive polynomial.

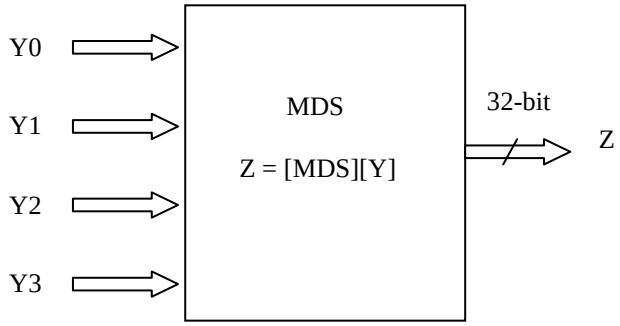

Fig 7: MDS block Diagram

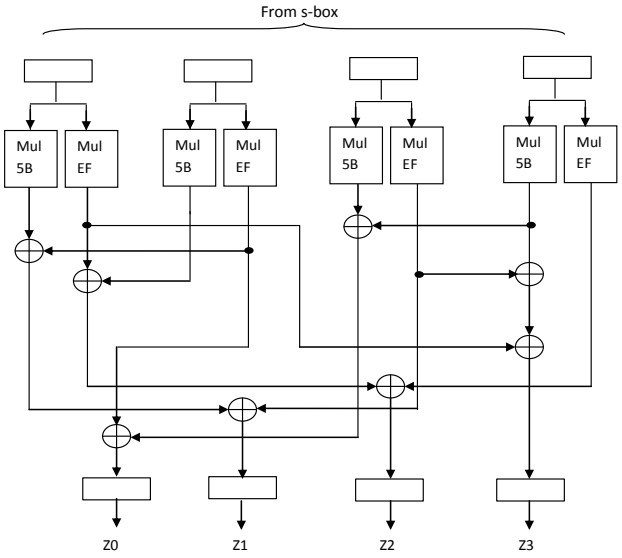

Fig 8: Modified MDS Block Diagram

A maximum distance separable (MDS) code over a field is a linear mapping from 'a' field elements to 'b' field elements, producing a composite vector of 'a + b' elements, with the property that the minimum number of non-zero elements in any non-zero vector is at least b+1. MDS mappings can be represented by an MDS matrix consisting of a x b elements.

z0 = EF_y1 + 5B_y2 + 5B_y3

z1 = 5B_y0 + EF_y1 + EF_y2

z2 = EF_y0 + 5B_y1 + EF_y3

z3 = EF_y0 + EF_y2 + 5B_y3

4.4 PHT

PHT is a reversible transformation of a bit string that provides cryptographic diffusion. Pseudo-hadamard transform consists of two additions. SAFER Algorithm uses PHTs extensively for diffusion for the first time. Twofish uses a 32-bit PHT. Given two inputs, a and b, the 32-bit PHT is:

a' = a + b mod 2^{32}
b '= a + 2b mod 2^{32}

Both additions are implemented in the same way as ordinary addition modulo 2^{32}. Twofish uses a 32-bit PHT to mix the outputs from its two parallel 32-bit g functions. PHT Using shift operation, in this method of PHT two 32-bit inputs are given, say in1 and in2 as shown in Fig 9. Here for the operations of equations shown below, are performed using the shifting. The function can be easily explained with the help of the following equations:

For out1 out1 = in1 + in2
For out2 out2 = in1 + in2x (i)
Where: In2x (i) = in2 (i - 1)
For i = 1 to 31
in2x(0) = 0 For i = 0

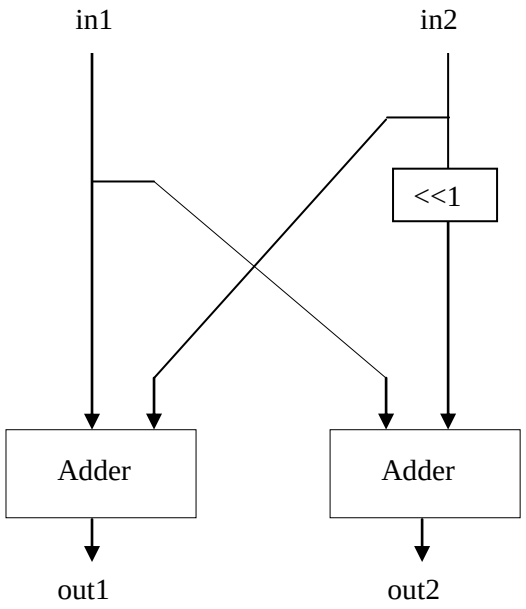

Fig 9 Architecture of PHT using shifting operation

5. Encryption and Decryption

Encryption means the art and science of secret writing. It stores and transmits the information safely over the insecure medium like Internet by encoding plain text into cipher text with the help of various encryption algorithms [10]. In twofish algorithm, for encryption, firstly, a 128-bit input plaintext P is divided into four parts of 32-bit each, say P0, P1, P2, P3 and XORed with four 32-bit sub-keys, K0, K1, K2, K3, as shown in Fig 2, then sixteen rounds of iteration and then the four outputs are Xor-ed with four more keys K4, K5, K6, K6. The resultant output is the 128-bit cipher-text. Decryption means the insecure medium like Internet by encoding plain text into cipher text with the help of various encryption algorithms. The decryption procedure of Twofish can be done in the same way as the encryption procedure by reversing the order of the sub-keys, which is one of merits of Feistel networks.

6. Results

The delay and frequency for encryption, decryption and for all the modules, for 128-bit twofish algorithm and 128-bit modified twofish algorithm is shown in Table 1. The delay and frequency for encryption, decryption and for all the modules, for 192-bit twofish algorithm and 192-bit modified twofish algorithm is shown in Table 2.

7. Conclusion and Future work

Twofish is a very flexible deign. From the sub-key generation to the data encryption, twofish offered a wide variety of design possibilities, which is actually one of its main advantages over its competitors. In this paper, twofish algorithm is studied and some modules have been modified keeping delay as main constraint. VHDL description of twofish, has been verified by functional simulation, using Xilinx xst-6.1, 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.

8. 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

[5] 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

[6] 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

[7] G. Catalini, F. Chiaraluce, L. Ciccarelli, E. Gamhi, P. Pierleoni, M. Reginelli, "modified twofish algorithm for increasing security and efficiency in the encryption of video signals" in IEEE, 2005

[8] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson,Tadayoshi Kohno, Mike Stay "The Twofish Team's Final Comments on AES Selection"

[9] Rabie A. Mahmoud1, Magdy Saeb2, "A Metamorphic-Enhanced Twofish Block Cipher And Associated FPGA Implementation" in The International Journal of Computer Science and Communication Security (IJCSCS), Volume 2, January 2012

[10] V. Mnssvkr Gupta, K.V.S. Murthy, A. Yesubabu, R. Shiva A Shankar, "Recent performance evaluation among various AES algorithm- MARS, RC6, RIJNDAEL, SERPENT, TWOFISH" in *International Journal of Science and Advanced Technology*, 2012

Table 1. Delay and frequency of twofish algorithm (128-bit)

Parameters	Twofish algorithm (128-bit)		Modified twofish algorithm (128-bit)	
	Delay (ns)	Frequency (MHz)	Delay (ns)	Frequency (MHz)
Function F	104.102	9.605	92.186	10.847
Function g	39.383	25.391	39.284	25.455
MDS	15.524	64.416	13.706	72.960
PHT	67.850	14.736	61.172	16.347
Encryption	105.794	9.453	93.878	10.652
Decryption	105.794	9.453	93.878	10.652

Table 2. Delay and frequency of twofish algorithm (192-bit)

Parameters	Twofish algorithm (192-bit)		Modified twofish algorithm (192-bit)	
	Delay (ns)	**Frequency (MHz)**	**Delay (ns)**	**Frequency (MHz)**
Function F	113.822	8.785	101.789	9.824
Function g	49.076	20.376	48.887	20.455
MDS	15.524	64.416	13.706	72.960
PHT	67.850	14.738	61.172	16.347
Encryption	115.307	8.672	103.481	9.663
Decryption	115.307	8.672	103.481	9.663