Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Performance Analysis of Secure Integrated Circuits using Blowfish Algorithm

V. Kumara Swamy[1], V. Kumara Swamy[2] and Dr. Prabhu Benakop[3]

[1] Auroras Engineering College

Received: 12 December 2012 Accepted: 2 January 2013 Published: 15 January 2013

Abstract

Security is an essential feature of Information Communication Technology (ICT). Information has to be encrypted at the transmitter side to maintain secrecy and decrypted at the receiver side to retrieve the original information for secure data transmission over insecure computer data communication networks. This paper analyzes the performance metrics of blowfish algorithm with and without Wave Dynamic Differential Logic (WDDL) style to incorporate security against differential power analysis. It compares Encryption Time (Et), Decryption Time (Dt) and Total Time (Tt) of Blowfish, Modified Blowfish with and without WDDL logic for secure Integrated Circuits (SIC) [7, 8]. Modified Blowfish with and without WDDL logic yielded good results compared to Blowfish with and without WDDL logic implementation . This paper is implemented using Xilinx webpack9.2i with Verilog Hardware Description language (HDL).

Index terms— ICT, WDDL, SIC, bf, et, Dt, dpa and hdl.

In the evaluation phase, each input signal is differential and the WDDL gate calculates its differential output. In the precharge phase, the inputs to the WDDL gate are set at 0. This puts the output of the gate at 0. During the precharge phase, the input vector of the combinatorial logic is set at all 0s. Each individual gate will eventually have all its inputs at 0, evaluate its output to 0, and pass this 0 value to the next gate. One could say that the precharge signal travels over the combinatorial logic as a 0-wave, hence, WDDL. They produce an all-zero output in the precharge phase (clk-signal high) but they produce actual logic when they it is let the differential signal through during the evaluation phase (clk-signal low). Comparing symmetric key algorithms, BF algorithm is fast, more secure with large key size and its chosen as choice of cryptographic algorithm to implement secure ICs against Differential Power Analysis (DPA) attack [10,11] using Wave Dynamic Differential Logic (WDDL).

In fig no.3, when clock is precharge mode (high), output is zero for both. When clock is evaluation mode (low), outputs are complemented and worked as XOR and XNOR.

1 b) Blowfish Algorithm

Blowfish is a 64-bit block cipher [1,2] presented by Bruce Schneider and is a suggested replacement for DES (Data Encryption Standard). DES was the standard cryptographic algorithm for more than 19 years, but it is now accepted that its key size is too small for present usage. It has a variable-length key block cipher of up to 448 bits. Although a complex initialization phase is required, the encryption of data is very efficient. It suits applications where the key does not change often.

WDDL can be implemented for any logic design. Since the discussion moves around crypto processors, it would be wise to consider a cryptographic algorithm called Blowfish is a fast algorithm [3,8].

2 II.

3 Analysis of Blowfish Algorithm

4 b) Substitution Boxes (S-boxes)

A substitution box (or S-box) is a basic component of symmetric key algorithm used to obscure the relationship between the plaintext and the cipher text In general, an S-box takes some number of input bits, 8_bit, and transforms them into some number of output bits, 32_bit: an 8×32 S-box, implemented as a lookup table [1,3,8] c) Feistel Function Block

5 d) Modulo 32-bit adder

To increase the speed of blowfish adders in this fig no.8 can be operated in parallel. one adder adds Two h-bit residues, X and Y to form their sum S1+2hCout1 .Another one is 3-operand adder that computes "X+Y+m". Note that if m=2n+1, we have h=n+1.It has been reported that if either Cout1 or Cout2 of this addition is '1' then the output is X+Y+m instead of X+Y. However, in the following we illustrate that only if the carry of "X+Y+m" is '1', it is sufficient to select it as the final output [4,9] The sub-key generation unit expands the given 448-bit key into 14 sub-keys and 4 more subkeys are internally generated, each of 32 bits, so that they can be used at different stages in the algorithm. The sub key generation process is designed to preserve the entire entropy of the key and to distribute that entropy uniformly throughout the sub keys. It is also designed to distribute the set of allowed sub keys randomly throughout the domain of possible sub keys. Then bit wise XOR of the P-array and K-array is performed reusing the words from K-array as needed shown in equation no.3. P 1 = P 1 ^K ? P 14 = P 14 ^K 14 P 15 = P 15 ^K 1 ? P 18 = P 18 ^K 4 -

IV.

6 Results and Discussion

Encryption consists of sixteen rounds of operations. Each round-one operation consists of xor, 8-Volume XIII Issue XVII Version I The encryption and decryption modules are integrated in the top level module to obtain the blowfish crypto-processor and the simulation results are analyzed.

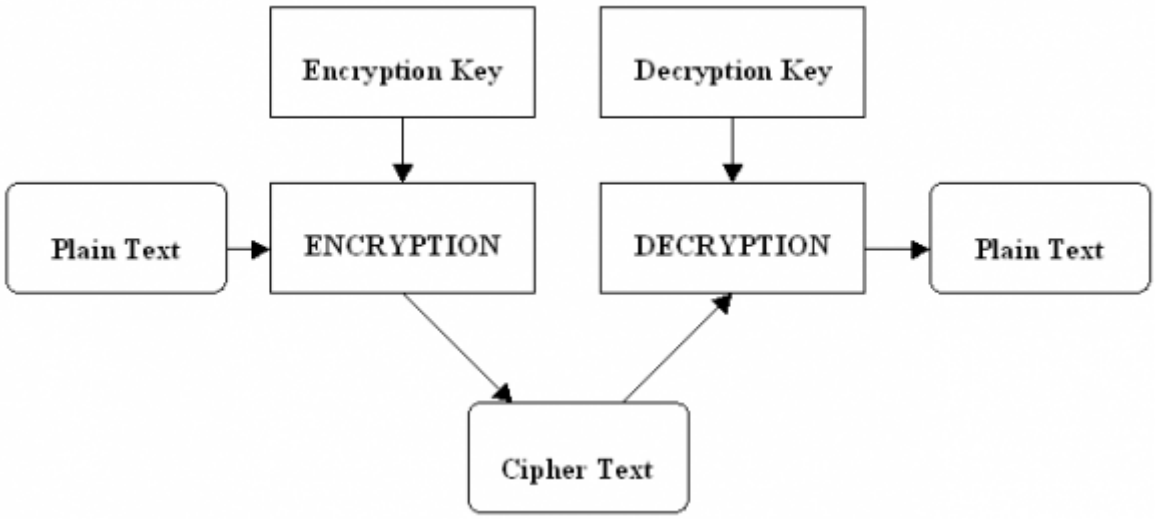
Blowfish Algorithm is implemented in four forms and compared its performance parameters which are given below in the table no.1 and the modified blowfish is producing better results than the normal blowfish. Analysis is done for blowfish with and without WDDL logic to secure the ICs against DPA attack by the hackers.

Comparison of Blowfish, modified Blowfish with and without WDDL logic is given below in the table no.1 and the corresponding bar charts are shown in the fig no.9, 10 and 11 for performance parameters Et, Dt and Tt respectively. Et: Encrypt Time, Dt: Decrypt Time, Tt: Total Time

7 Conclusion

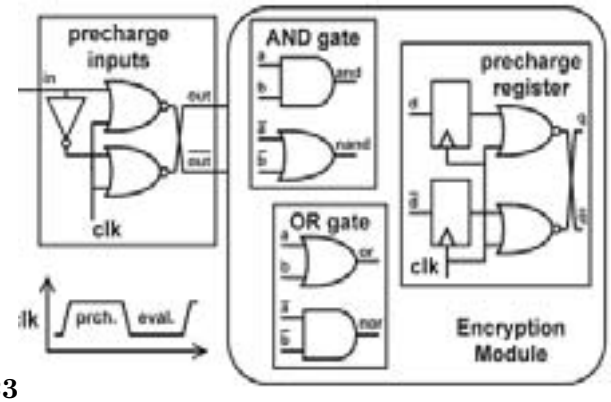
In this paper, an implementation of Blowfish Algorithm is designed using WDDL Logic style. In the implementation bottom-up approach is used. The subkeys generated for a particular key can be used for the encryption of the entire data to be encrypted with that key. The sub keys are given in reverse direction of the decryption data path without changing the design for decryption. The crypto processor has been designed for the key size of 448 bits and plain text of 64 bits. The code for the implementation has been written in Verilog HDL. The functional verification has been done using the ModelSim 5. [1] [2]

Figure 1: Introduction



1

Figure 2: Figure 1 :



23

Figure 3: Figure 2 :Figure 3 :

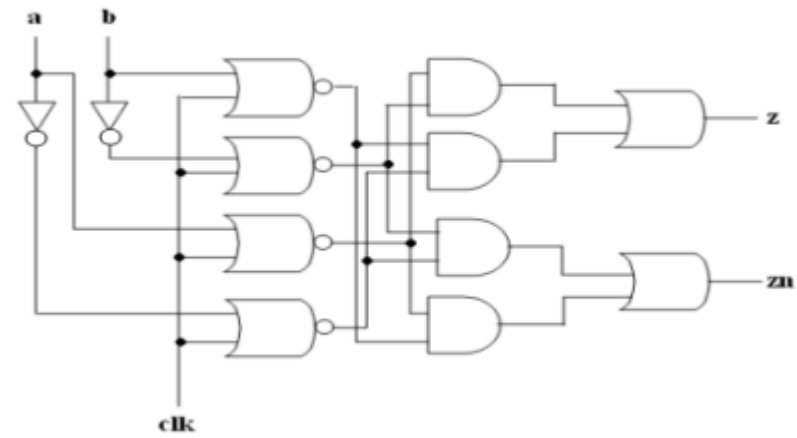


Figure 4: E

For i = 1 to 16 do

$RE_i = LE_{i-1} \oplus P_i$;

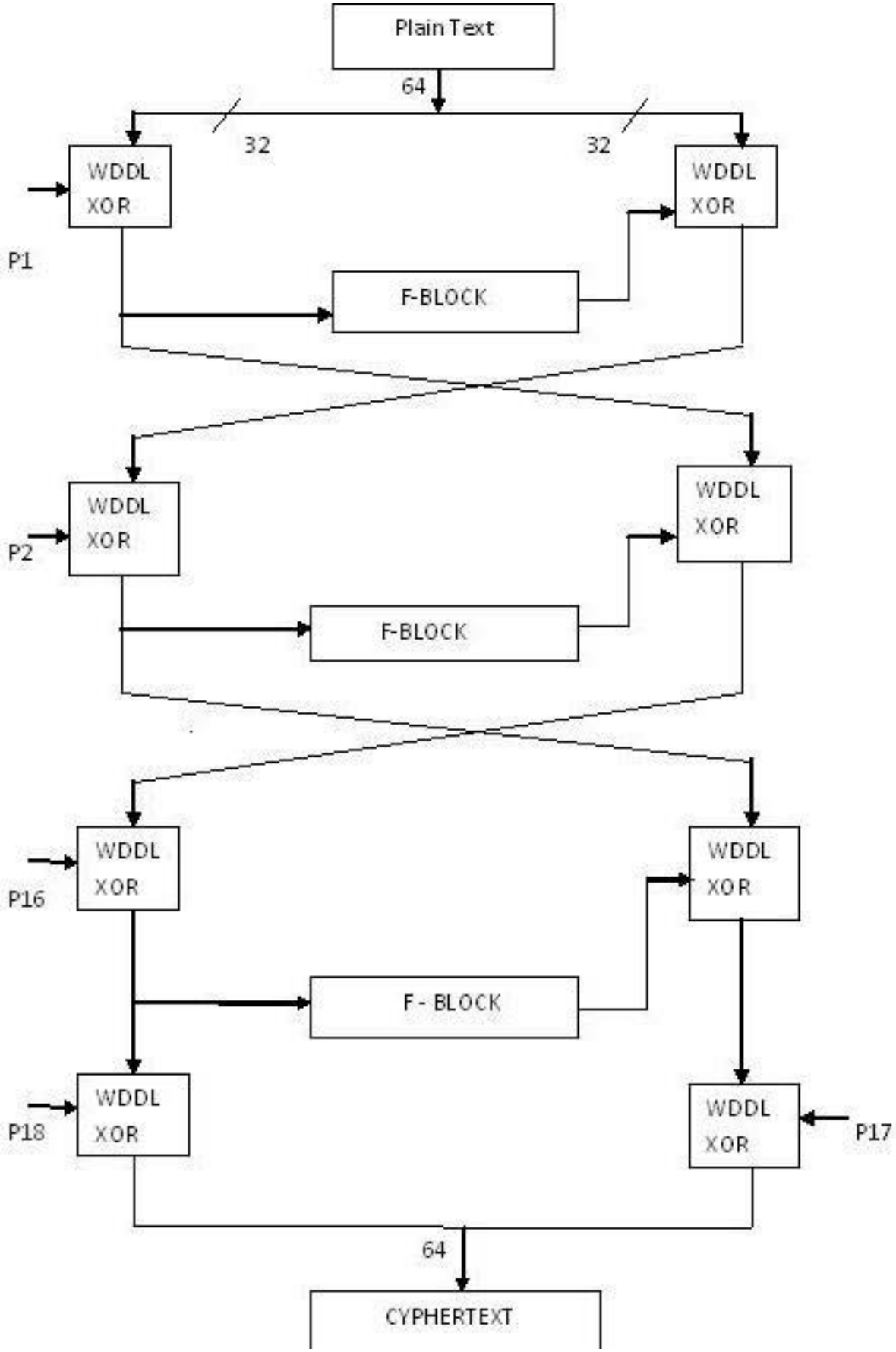
$LE_i = F[RE_i] \oplus RE_{i-1}$;

$LE_{17} = RE_{16} \oplus P_{18}$;

$RE_{17} = LE_{16} \oplus P_{17}$;

6

Figure 5: Figure 6 :



7

Figure 6: Figure 7 :

For $i = 1$ to 16 do

$RD_i = LD_{i-1} \oplus P_{19-i}$

$LD_i = F[RD_i] \oplus RD_{i-1}$;

$LD_{17} = RD_{16} \oplus P_1$;

$RD_{17} = LD_{16} \oplus P_2$;

8

Figure 7: Figure 8 :

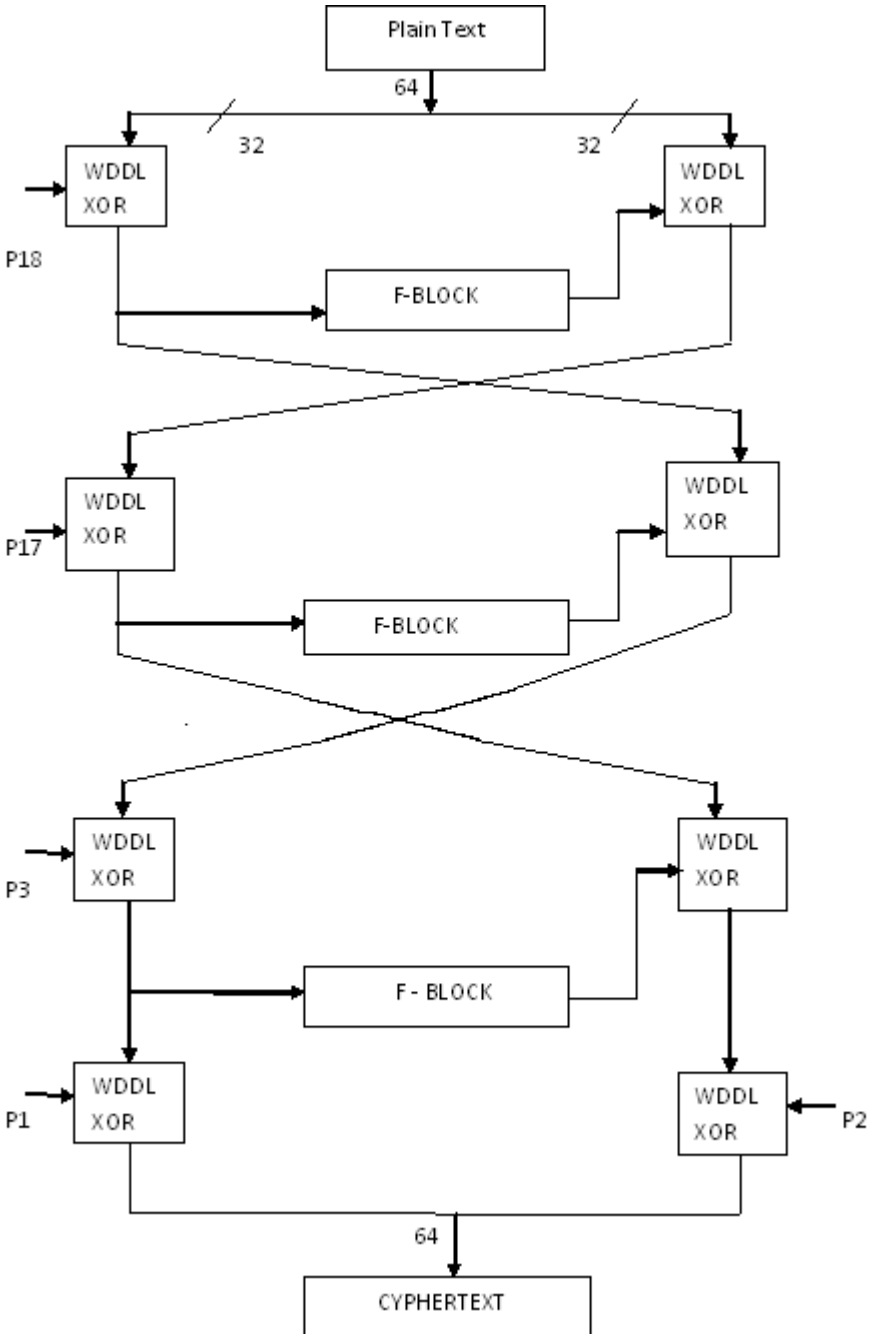
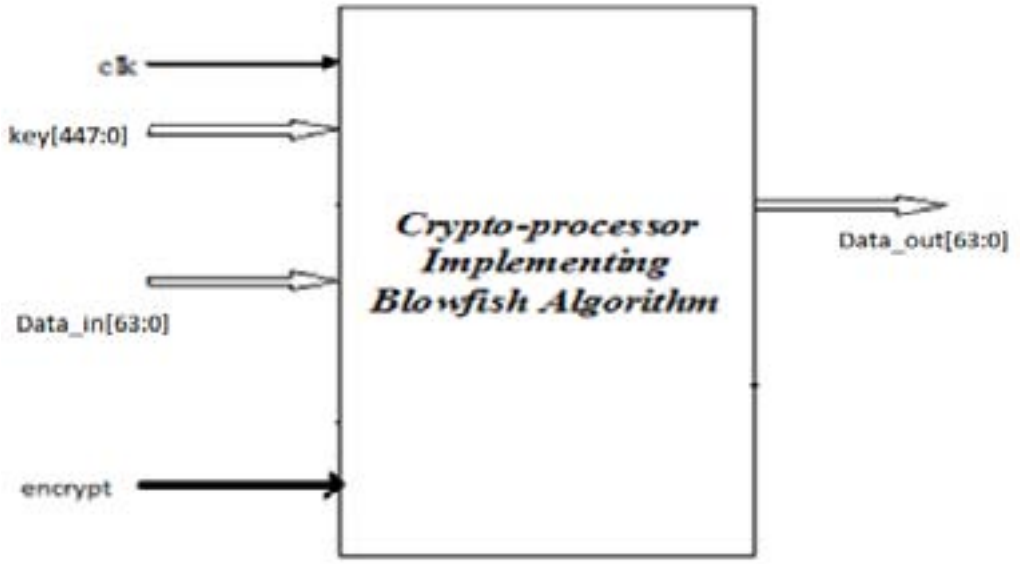


Figure 8:



91011

Figure 9: Figure 9 :Figure 10 :Figure 11 :

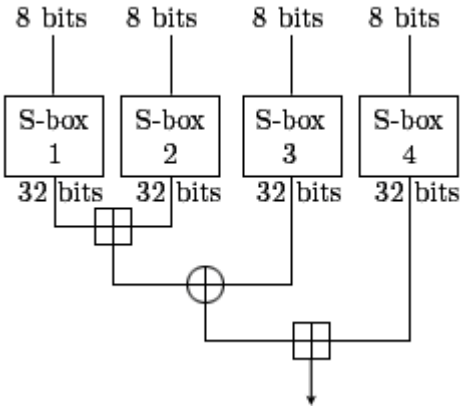


Figure 10:

1

S No	Name of Crypt-algorithm	Performance parameters Et(ns)	Dt(ns)	Tt(ns)
1	Blowfish	98.663	98.663	99.395
2	Modified Blowfish	70.08	70.08	71.067
3	Blowfish with WDDL	107.62	107.62	112.56
4	Modified Blowfish with WDDL	73.985	73.985	76.337

Figure 11: Table 1 :

[Singh and Kumar Singla] , Gurjeevan Singh , Ashwani Kumar Singla .

[TRANSACTIONS ON COMPUTERS ()] , *TRANSACTIONS ON COMPUTERS* FEBRUARY 2012. 61 (2) .

[Tiri et al. (2006)] 'A Digital Design Flow for Secure Integrated Circuits'. Kris Tiri , Ieee Member , Ingrid Verbauwhede , Senior Member . *IEEE Transaction on Computer-Aided Design of Integrated Circuits and Systems* July 2006. IEEE. 25 (7) .

[Tiri and Verbauwhede ()] 'A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation'. K Tiri , I Verbauwhede . *Proc. Design, Automation and Test Eur. Conf. (DATE)*, (Design, Automation and Test Eur. Conf. (DATE)Paris, France) 2004. p. .

[Agrawal and Mishra (2012)] 'A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm'. Monika Agrawal , Pradeep Mishra . *International Journal of Engineering and Advanced Technology (IJEAT)* 2249 -8958. August 2012. (1) .

[Walied et al. (2012)] 'An Implementation of High Security and High Throughput Triple Blowfish Cryptography Algorithm'. W Walied , Ali E Souror , Rasheed Taki El-Deen , Adel Mokhtar -Awady Ahmed , Zaghlul-mahmoud . *International Journal of Research and Reviews in Signal Acquisition and Processing (IJRRSAP)* 2046-617X. March 2012. 2 (1) .

[Liu et al. ()] 'Critical Path Based Hardware Acceleration for Cryptosystems'. Chen Liu , Rolando Duarte , Omar Granados , Jie Tang , Shaoshan Liu , Jean Andrian . *Journal of Information Processing Systems* 2012. 8 (1) p. . (JIPS))

[Swamy et al. ()] 'Design and Implementation of DPA Resistant Crypto-Processor using Blowfish Algorithm'. V Kumara Swamy , Dr Prabhu , G Benakop , P Sandeep . *International Conference on Advanced Communication and Informatics (ICACI-2009)*, (TPGIT, Vellore, Tamilnadu, India) January 11,12, &13th, 2009. p. .

[Swamy et al. ()] 'Implementation of digital design flow for DPA secure WDDL crypto processor using blowfish algorithm'. V Kumara Swamy , G Prabhu , B Benakop , Sandeep . *The Libyan Arab International Conference on Electrical and Electronic Engineering (LAICEEE-2010)*, (Tripoli, Libya) October 23-26, 2010. p. .

[Timarchi and Navi ()] 'Improved Modulo 2n +1 Adder Design'. Somayeh Timarchi , Keivan Navi . *International Journal of Computer and Information Engineering* 7 2008. 2.

[Haridimos et al.] *On Modulo 2n +1 Adder Design*, T Haridimos , Giorgos Vergos , Dimitrakopoulos . IEEE.

[Pavithra et al. (2012)] 'Study and Performance Analysis of Cryptography Algorithms'. S Pavithra , . E Mrs , Ramadevi . *International Journal of Advanced Research in Computer Engineering & Technology* July 2012. 1 (5) .

[Sandha (2011)] *Through Put Analysis of Various Encryption Algorithms*, K S Sandha . September 2011. 2 p. e3. (IJCST)