Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 17 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Analysis of Secure Integrated Circuits using Blowfish Algorithm

By V. Kumara Swamy & Dr. Prabhu Benakop
Auroras Engineering College, India

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).

Keywords: ICT, WDDL, SIC, bf, et, Dt, dpa and hdl.

GJCST-E Classification : C.4

Strictly as per the compliance and regulations of:

Performance Analysis of Secure Integrated Circuits using Blowfish Algorithm

V. Kumara Swamy [α] & Dr. Prabhu Benakop [σ]

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).

Keywords: ICT, WDDL, SIC, bf, et, Dt, dpa and hdl.

I. Introduction

The original information is known as plaintext, and the encrypted form as ciphertext. The ciphertext message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it. It is varied depending on a key this change the detailed operation of the algorithm. As shown in the fig no.1, at the encryption we apply plaintext and key as inputs and it produces ciphertext. At the other end, ciphertext and key are the inputs to decryption and the result is the recovery of original plaintext. It is a symmetric key algorithm.

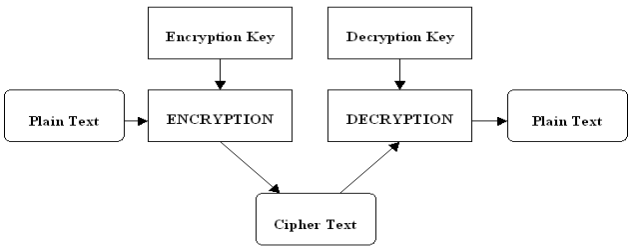

Figure 1 : Symmetric Key Encryption and Decryption

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).

Authors α σ: ECE, Aurora's Engineering College, Bhongir, Nalgonda Dist, A.P., India. e-mails: ksvarkuti@yahoo.com, pgbenakop@ieee.org

a) Wave Dynamic Differential Logic (WDDL)

WDDL logic consists of a parallel combination of two positive complementary gates, one calculating the true output using the true inputs, the other the false output using the false inputs. A positive gate produces a zero output for an all zero input. The AND gate and the OR gate are examples of positive gates. The AND gate fed with true input signals and the OR gate fed with false input signals are two dual gates. Fig.no.2 shows the WDDL AND gate and the WDDL OR gate. 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).

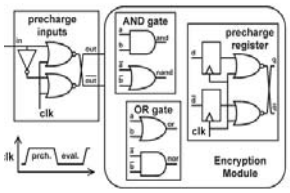

Figure 2 : Wddl and/or Gate With Precharge Circuit

WDDL logic is a constant power consumption logic which can overcome the DPA attack by the hacker. During the Precharge phase, the normal and complemented outputs of the digital circuit produce equal outputs. Thus the differential power analysis results in zero differential power to not to allow the hacker to gain the information from the hardware integrated circuits. During evaluation phase, it generates actual outputs as per logic with correct key.

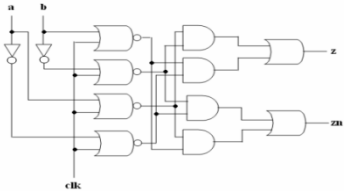

Figure 3 : Wddl Xor Gate

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.

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].

II. Analysis of Blowfish Algorithm

Blowfish is a symmetric block cipher that encrypts and decrypts data in 8-byte (64-bit) blocks. The algorithm has two parts, key expansion and data encryption. Key expansion consists of generating the initial contents of one array (P-array), namely, eighteen 32-bit sub-keys, and four arrays (the S-boxes), each of size 256 by 32 bits, from a key of at most 448 bits (56 bytes). The data encryption and Decryption uses a 16-round Feistel Network as shown below in fig no.4 and fig no.5 [7, 8].

The encryption algorithm can be defined by the following pseudo code equation no.1:

$$\begin{aligned} &\text{For } i = 1 \text{ to } 16 \text{ do} \\ &\quad RE_i = LE_{i-1} \oplus P_i; \\ &\quad LE_i = F[RE_i] \oplus RE_{i-1}; \\ &LE_{17} = RE_{16} \oplus P_{18}; \\ &RE_{17} = LE_{16} \oplus P_{17}; \end{aligned} \quad (1)$$

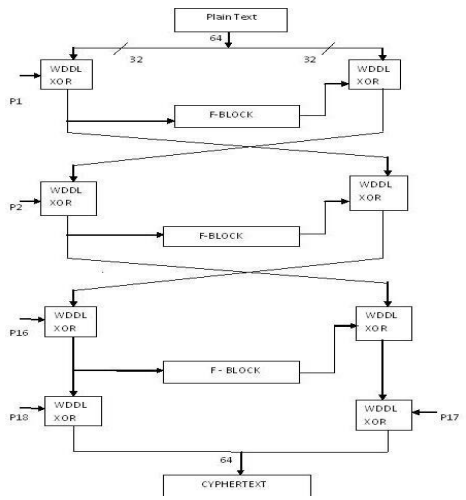

Figure 4 : Blowfish Encryption

The Decryption algorithm can be defined by the following pseudo code equation no.2:

$$\begin{aligned} &\text{For } i = 1 \text{ to } 16 \text{ do} \\ &\quad RD_i = LD_{i-1} \oplus P_{19-i} \\ &\quad LD_i = F[RD_i] \oplus RD_{i-1}; \\ &LD_{17} = RD_{16} \oplus P_1; \\ &RD_{17} = LD_{16} \oplus P_2; \end{aligned}$$

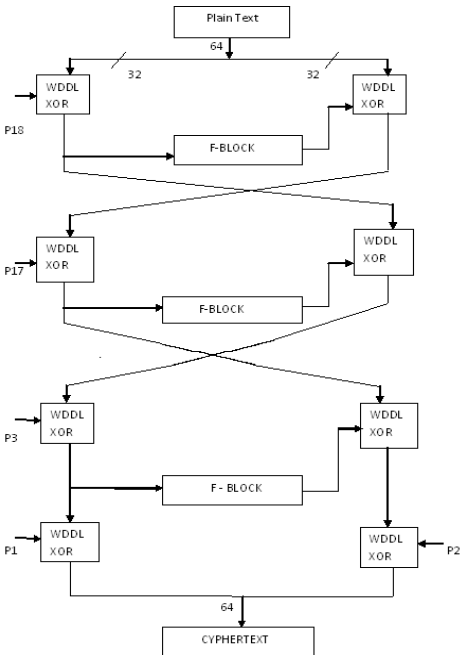

Figure 5 : Blowfish Decryption

III. Design of Blowfish Algorithm

Secure crypto processor is a dedicated computer or microprocessor for carrying out cryptographic operations, embedded in a packaging with multiple physical security measures. The purpose of a secure crypto processor is to act as the keystone of a security sub-system, eliminating the need to protect the rest of the sub-system with physical security measures. Smartcards are probably the most widely deployed form of secure crypto processor, although more complex and versatile secure crypto processors are widely deployed in systems such as Automated teller machines, TV set-top boxes, and high-security portable communication equipment. A crypto processor implementing Blowfish algorithm may be shown in fig no.6.

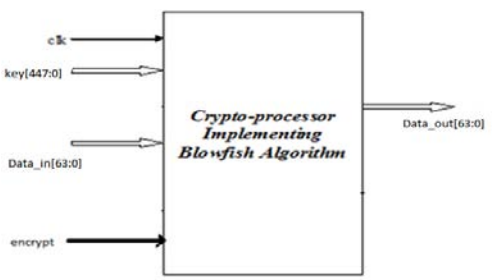

Figure 6 : Blowfish Crypto-processor

a) Description of the signals

Clk: The input clock signal.

Key[447:0]: The encryption/decryption key. If less than a 448-bit key is desired, this signal must be padded up to 448 bits. Typically, this padding consists of all 0's.

data_in[63:0]: The input data. In encryption mode, this is the plaintext. In decryption mode, this is the cipher text. This is only read when the ready signal is asserted.

data_out[63:0]: The output data. In encryption mode, this is the cipher text. In decryption mode, this is the plaintext. This is only modified during key initialization and the same cycle that ready is raised after an encryption or decryption sequence.

Encrypt: This signal toggles between encryption and decryption operation. 1 means encrypt, 0 means decrypt.

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

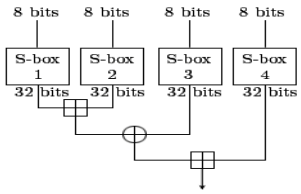

Figure 7 : Function Block Internal Structure

Function 'F' is used to create 'confusion' to thwart cryptanalysis based on statistical analysis. 'Confusion' seeks to make the relationship between the statistics of the cipher text and the value of encryption key as complex as possible. One advantage of this model is that the round function F does not have to be invertible, and can be very complex as shown in fig no.7 [1, 3, 8].

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]

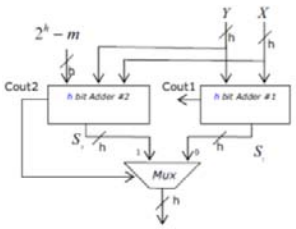

Figure 8 : Modulo M –bit adder

e) Sub-key Generation Unit

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.

$$P_1 = P_1 \wedge K \ldots P_{14} = P_{14} \wedge K_{14}$$
$$P_{15} = P_{15} \wedge K_1 \ldots P_{18} = P_{18} \wedge K_4 - \quad (3)$$

IV. Results and Discussion

Encryption consists of sixteen rounds of operations. Each round-one operation consists of xor, 8-bit to 32-bit substitution, 32-bit modulo addition, xor, 32-bit modulo addition and swapping of result of Left Encryption (LE) to Right side and Right Encryption (RE) to left side of the data flow as shown in fig no.6. After performing 16 round-one operations right side output[31:0] xored with subkey p16[31:0] and left hand side output[31:0] xored with subkey p17[31:0] and then we get final cipher text[63:0].

Decryption is same as that of encryption except we applied subkeys p0 to p17 in reverse order. Input data is the ciphertext (output of encryption) and then we get the output as Plaintext. Decryption consists of sixteen- round one operation. Each round-one operation consists of xor, 8-bit to 32-bit substitution, 32-bit modulo addition, xor, 32-bit modulo addition and swapping of result of Left Encryption (LE) to Right side and Right Encryption (RE) to left side of the data flow as shown in fig no.7. The input data ciphertext[63:0] performs 16 round-one operations with 16 sub keys(p17 to 2) and then after performing 16 round-one operations right side output[31:0] xored with subkey p1[31:0] and left hand side output[31:0] xored with subkey p0[31:0] and then we get final plaintext.

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.

Table 1 : Comparison of four implementations of Blowfish Algorithm for Et, Dt and Tt

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

Et: Encrypt Time, Dt: Decrypt Time, Tt: Total Time

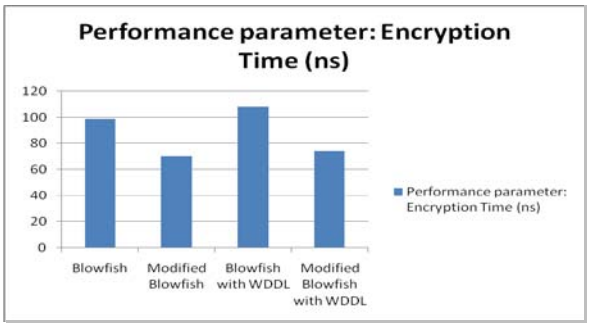

Figure 9 : Bar Chart for Performance parameter Encryption Time of four implementations of Blowfish Algorithm

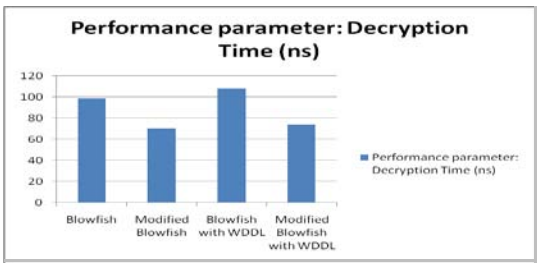

Figure 10 : Bar Chart for Performance parameter Decryption Time of four implementations of Blowfish Algorithm

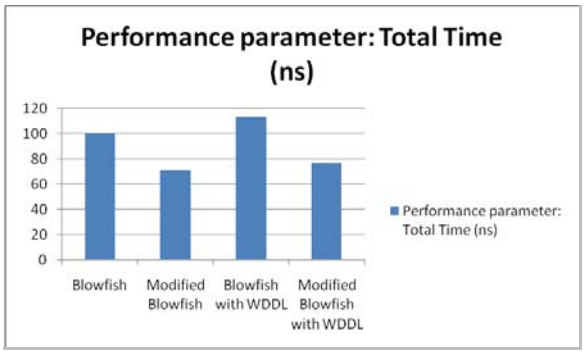

Figure 11 : Bar Chart for Performance parameter Total Time (i.e., Propagation Delay) of four implementations of Blowfish Algorithm

V. Conclusion

In this paper, an implementation of Blowfish Algorithm is designed using WDDL Logic style. In the implementation bottom-up approach is used. The sub-keys 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 5.5 simulation package. The synthesis of the design is done using the Xilinx Web Pack9.2i. Comparison with different implementations has been given in table no.1 and proved that Modified Blowfish with and without WDDL logic yielded the best results in Encryption time, Dectryption time and Total Propagation delay compared to blowfish with and without WDDL logic respectively.

References Références Referencias

1. Monika Agrawal, Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-6, August 2012.
2. S. Pavithra, Mrs. E. Ramadevi," Study and Performance Analysis of Cryptography Algorithms", International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012.
3. Walied W. Souror, Ali E. Taki el-deen, Rasheed Mokhtar -awady Ahmed, Adel ZaghlulMahmoud ,"An Implementation of High Security and High Throughput Triple Blowfish Cryptography Algorithm" International Journal of Research and Reviews in Signal Acquisition and Processing (IJRRSAP)Vol. 2, No. 1, March 2012, ISSN: 2046-617X.
4. Haridimos T. Vergos, Giorgos Dimitrakopoulos, "On Modulo 2n +1 Adder Design", IEEE

TRANSACTIONS ON COMPUTERS, VOL. 61, NO. 2, FEBRUARY 2012.

5. Chen Liu, Rolando Duarte, Omar Granados, Jie Tang, Shaoshan Liu, Jean Andrian., "Critical Path Based Hardware Acceleration for Cryptosystems," Journal of Information Processing Systems (JIPS), Vol. 8, No. 1, pp.133-144, 2012.
6. Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha, "Through Put Analysis of Various Encryption Algorithms", IJCST Vol.2, Issue3, September 2011.
7. V.Kumara Swamy, Prabhu G Benakop, B. Sandeep, "Implementation of digital design flow for DPA secure WDDL crypto processor using blowfish algorithm", The Libyan Arab International Conference on Electrical and Electronic Engineering (LAICEEE-2010), Tripoli, Libya, October 23-26, 2010, pp.565-73.
8. V.Kumara Swamy, Dr Prabhu G Benakop and P.Sandeep, "Design and Implementation of DPA Resistant Crypto-Processor using Blowfish Algorithm", International Conference on Advanced Communication and Informatics (ICACI-2009), TPGIT, Vellore, Tamilnadu, India, January 11,12, &13th, 2009, pp.25-32
9. Somayeh Timarchi, Keivan Navi, "Improved Modulo 2n +1 Adder Design", International Journal of Computer and Information Engineering 2:7 2008.
10. Kris Tiri, Member, IEEE, and Ingrid Verbauwhede, Senior Member, IEEE "A Digital Design Flow for Secure Integrated Circuits", IEEE Transaction on Computer-Aided Design of Integrated Circuits and Systems, Vol. 25, No. 7, July 2006.
11. K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation", in Proc. Design, Automation and Test Eur. Conf. (DATE), Paris, France, 2004, pp. 246–251.

This page is intentionally left blank