Available online at www.ejournals.uofk.edu

U of KEJ Vol. 8 Issue 1 pp. 25-30 (February 2018)

UNIVERSITY OF KHARTOUM ENGINEERING JOURNAL (UofKEJ)

A Compact Cryptosystem Design of Triple-DES

Murtada Mohamed Abdelwahab

Faculty of Engineering & Technology - Department of Electronic Engineering
University of Gezira
(E-MAIL: mortadamohammad@yahoo.com)

Abstract: Symmetric encryption algorithms are widely used in the field of information security due to the rapid increasing need to pass information via computer networks and communication technology. All symmetric algorithms are commonly used the same key for encryption and decryption. Triple-Data Encryption algorithm TDEA is a type of symmetric encryption methods. The proposed algorithm consists of triple-keys used through three stages of single round DES design. The proposed implementation in this paper is optimized in terms of chip area and performance speed. The results are concluded in terms of chip area performance and performance per area. The comparison results with similar encryption algorithms are satisfying and very competitive.

Key words: *TDEA, FPGA Performance, Encryption, Algorithm.*

I. INTRODUCTION

Cryptographic devices requirements of field programmability and various operational requirements call for a reduced space, weight, and power consumption. Field programmable gate arrays (FPGAs) are the future platform which is capable to address these requirements [1]. The proposed implementation in this paper is a very compact design of triple DES algorithm. It consists of three data encryption standard (DES) module which is created using single round of encryption. It is a fact that TDES is more secure than DES and about one third slower than single DES in terms of performance speed. There are a lot of applications that used information security algorithms are concerned for high speed with an appropriate level of security.

The implementation that presented here offers better results in terms of performance and effective area due to the using of compact architecture, which yields a short path of encryption and decryption. The design is implemented on different types of FPGA devices. Programmable logic blocks are the basic elements of FPGAs structure. This structure makes FPGA flexible to Perform any logic design. The main advantage of $FPGA_s$ technology that they have the ability to reprogram their logic blocks any time even on the system work. The logic blocks contains lookup tables (LUTs), flip- flops and switchable interconnect for the purpose of routing [2]. FPGAs have high demand for industrial use because it needs a short time before entering to market. Ddigital circuits designers have been become prefer it widely because they can make changes in their designs easily every time they need to [3].

2. TRIPLE DES ALGORITHM

Triple DES Algorithm was known in 1993. As shown in Fig.1 the TDEA block diagram performs a compound operation of DES. The standard specifies the following keying options for bundle (K1, K2, K3) [4]:

1. Keying Option 1: K1, K2 and K3 are independent keys.

2. Keying Option 2: K1 and K2 are independent keys and K3= K1.

3. Keying Option 3: K1= K2= K3.

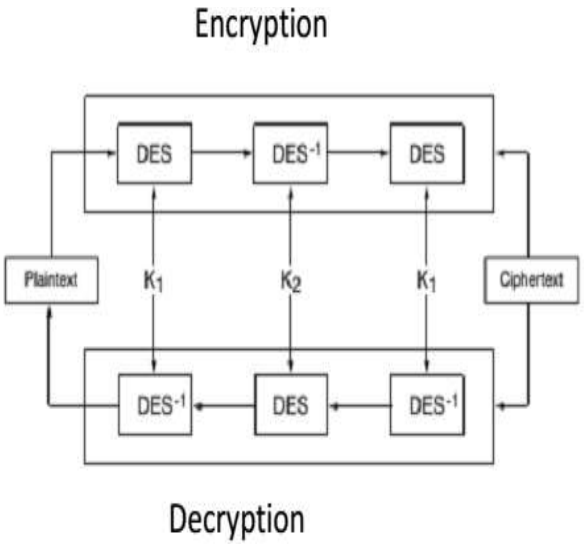


Fig.1. TDEA Block Diagram

The security options are greatest in the Keying Option 1 and less in the keying Option 2. Keying Option 3 is identical to single DES.

3. METHODOLOGY

The implementation scheme as shown in Fig.2 consists of three stages of DES. The design can be used either to perform the function of encryption or decryption by setting the required mode. The design flow steps starts by written a VHDL code then synthesize the code and then the final step is to place and route the synthesize code using ISE Xilinx software which is free available online. As it shown in this paper, each DES module has five inputs and two outputs.

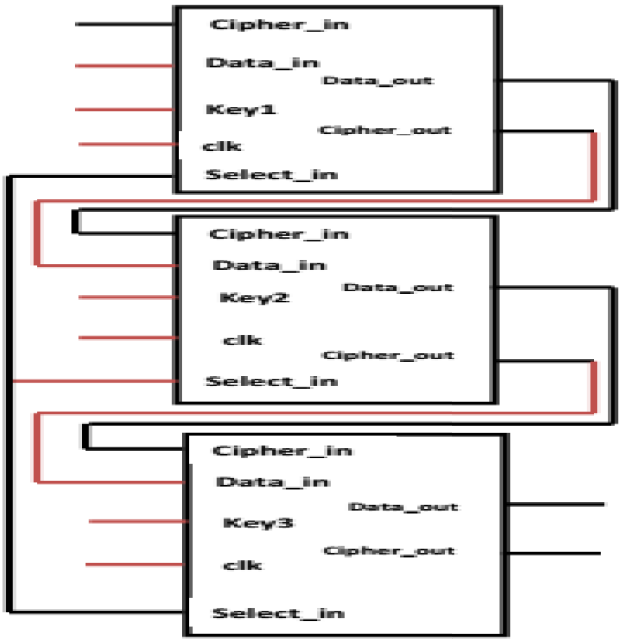


Fig.2. Triple –DES Operation Scheme

A. Key Generator

Generating the key in different forms is an extremely required operation for the purpose of providing high secure algorithm. The process that used for scheduling the 64 bit key is shown in Fig.3. Each input key pass through two steps:

1. Initial permutation: This operation responsible for dividing the 64 bit into 8 bytes expressed as:

$K = \quad k_1 \quad k_2 \quad k_3 \quad k_4 \quad k_5 \quad k_6 \quad k_7 \quad k_8$

The key divides into two registers:

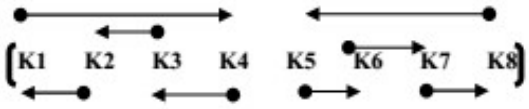
i. Right half key.

$K_5 \quad K_6 \quad K_7 \quad K_8$

ii. Left half key.

$K_1 \quad K_2 \quad K_3 \quad K_4$

2. Each byte of the right side is shifted to the right and each byte from the left side of the key is shifted to the left in a new place as shown in the following sketch:



This map applied to each input key of the three DES modules. The position of each byte in any input key depends on the previous position of the last key. The final result can be written as:

Key1=

$\{ K_2 \quad K_3 \quad K_4 \quad K_1 \quad K_8 \quad K_5 \quad K_6 \quad K_7 \}$

Key2=

$\{ K3 \quad K4 \quad K1 \quad K2 \quad K7 \quad K8 \quad K5 \quad K6 \}$

Key3=

$\{ K4 \quad K1 \quad K2 \quad K3 \quad K6 \quad K7 \quad K8 \quad K5 \}$

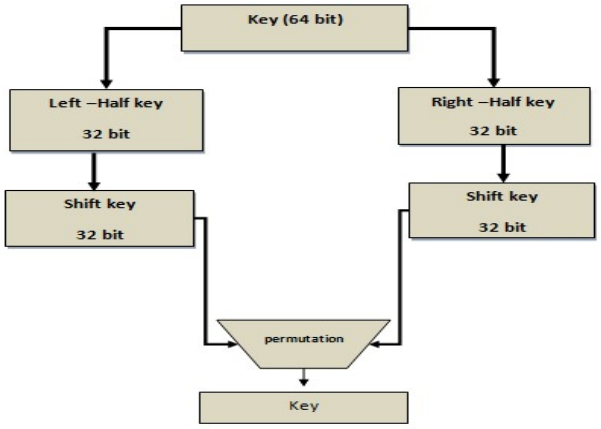


Fig.3. Key Function Generator

B. Encryption Algorithm

This implementation created in a very compact architecture to improve the performance speed and to have the possibility to implement it in several sizes of FPGA$_s$. The implementation architecture is specified as shown in Fig.4. This function called feistal network, as it shown the key scheduling is the essence of any encryption algorithm.

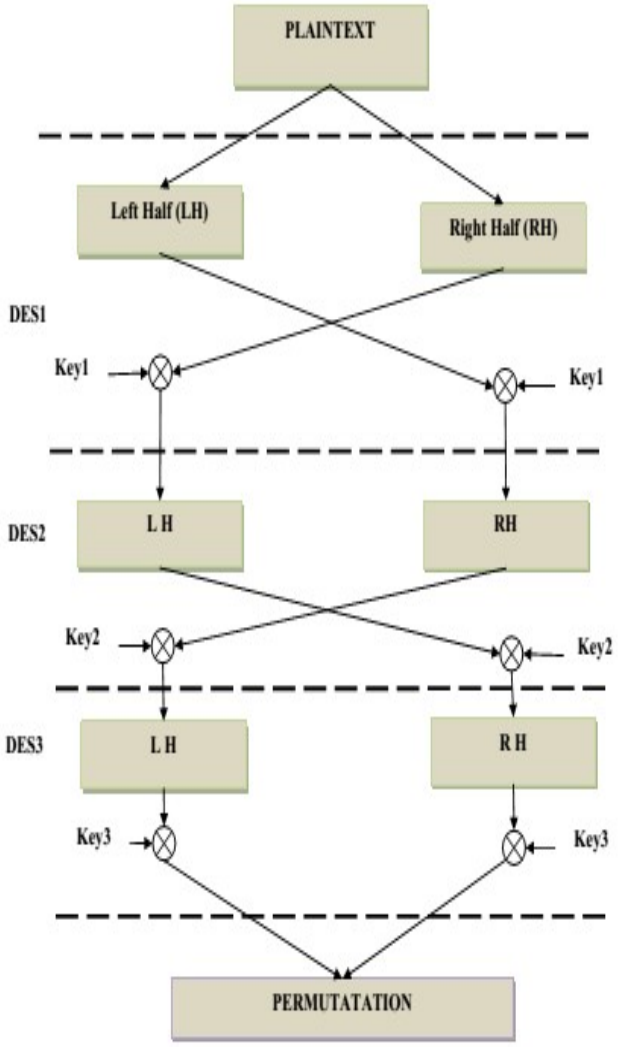


Fig.4. Triple DES Architecture

The structure composed of three DES modules, each DES module characterized by its short path of encryption or decryption, the system has single input key and the input data block encrypted with three keys generated using a key schedule process as discussed in the previous section. The size of data is 64 bit which added (xored) to each DES key where each DES module consist of one round of encryption. Decryption scheme is similar but it operates in a reverse map. The top view of the design demonstrates all inputs and outputs as shown in Fig.5.

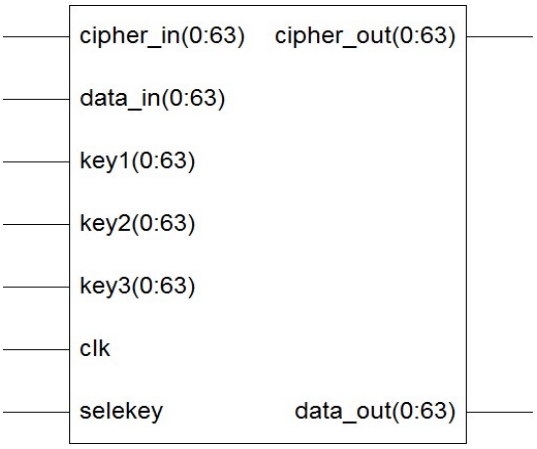


Fig.5. Inputs/Outputs Scheme

The interconnections of programmable logic blocks inside the FPGA device are shown in Fig. 6. This figure demonstrate the mechanism of place and route of connections and internal blocks such as flip flops ,registers etc.

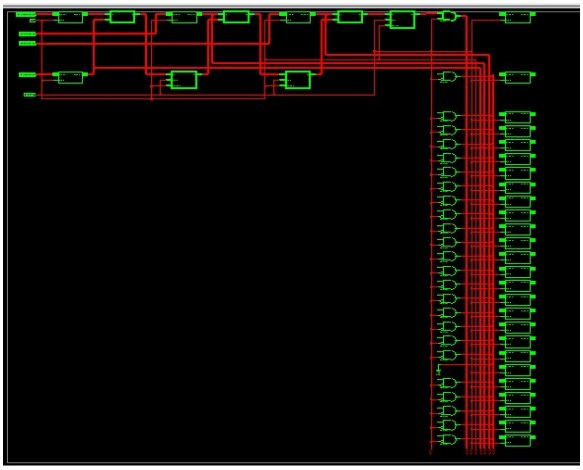


Fig.6. Technology Scheme

4. RESULTS AND DISCUSSION

The results shown in table I and table II are carried out using ISE9.1 Xilinx software. The synthesize process enables us to test the design in FPGA device and compared the results to other related implementations. The targeted FPGA device is spartan3.

Table 1. Coverage area of Spartan3

Xc3s4000-5fg676	
Parameter	**Used**
Number of slices	**386/27648**
Number of Flip Flop	**360/55296**
Number of 4 input LUTs	**481/55296**
Number of bonded IOB$_s$	442/489

Table 1: illustrates the amount of logics and slices

Required in implementing this design. It is shown that only 386 slices of the total area are used. Reducing the usage area and the amount of routing will help to reduce the delay time. The performance results are presented in table 2.

Table 2. Performance Results

Spartan -3 Speed Grade: -5	
Minimum period	2.057 ns
Maximum Frequency	486.180 MHz
Minimum input arrival time before clock	5.63 ns
Maximum output required time after clock	6.141 ns
Throughput	77.58 Mbps
Throughput/slice	0.2Mbps/slice

5. RELATED WORKS

Table III gives the performance and usage area of different encryption standards. This table illustrates the improvements offered by the proposed design in terms of throughput and utilizes area of the FPGA.

Table 3. Related Works

Design	Device used	Area	Frequency MH_Z	Throughput Mbps
Wong et al [9]	XC4020E	438	10	26.7
Neveen [8]	Xc3s200	359	----	----
Saqip et al. [10]	XCV400E	117	68.05	274
Ghosal et al [5]	XCV1600E	1481	-	-
Al Azad [6]	XCV1600E	645	-	
Antonios et al [7]	XCV1600E	12635	-	-
Aqib [12]	Vertex 5	887	-	-
Anton-ios **[7]**	Vertex E	1481	-	-

Wong et al [9] and saqip et al [10] both presented compact design consisting of single round of encryption. Ghosel[5] and Al-Azad[6] proposed TDES algorithm. Aqib [12] covers DES and Triple DES algorithm with Cipher Block Chaining concept basic on FPGA technology and implemented using Verilog in vertex FPGA. It consists of 16 rounds.

4. CONCLUSIONS

The paper proposed a compact design of TDES algorithm. The results indicated better usage of the FPGA resources as compared to other TDES algorithms but it is still slower than other encryption algorithms such as AES and DES. The results of comparison with existing implementations show that the proposed design is more efficient in most aspects.

REFERENCES

[1] Tony .H, "High-Assurance, High-Performance, High-Level Design with Cryptol", The National Security Agency's Review of Emerging Technologies,Vol(19) No(1),2011.

[2] Ted.H, Cythia.I, Thuy.D.N, Temothy.L, Ryan.K, Temothy. S. "Handbook of FPGA Design Security", New York, USA, Springer.2010.

[3] Dimitrios.M, Ioannis.P. Power consumption estimations vs measurements for FPGA-based security cores". In IEEE (2008) International Conference on Reconfigurable Computing and FPGAs, pp 433- 437, Cancun, Mexico 2008.

[4] Vikram.P, Steve.T" High-Speed DES and Triple DES Encryptor/Decryptor"xilinix journal, v1.0, 2001.

[5] P.Ghosal and M.Biswas,"A Compact FPGA Implementation of Triple DES Encryption System with IP Core Generation and On-Chip Verification. In: IEEE2010 Industrial Engineering and Operations Management Conference, Dhaka, Bangladesh, pp 339-345, January2010.

[6] Al Azad.A," Efficient VLSI Implementation of DES and Triple DES Algorithm with Cipher Block Chaining concept using Verilog and FPGA", International Journal of Computer Applications, Vol(44),No(16),pp:615, 2012.

[7] Antonios.F, Nikolaos.P, Panagiotis.M, and Emmanouel.A, "Hardware Implementation of Triple-DES Encryption/ Decryption Algorithm", International Conference on Telecommunications and Multimedia, 2006.

[8] Naveen .K and Gopal .V "VLSI Implementation of Data Encryption Standard Algorithm" International Journal of Innovative Technology and Exploring Engineering (IJITEE), PP: 106-110, Volume-1, Issue-6, November 2012.

[9] Wong.K, Wark.M, Dawson.E, "A single-chip FPGA implementation of the data encryption standard (DES) algorithm,"IEEE Globecom Communication, vol.2, pp. 827-832, Sydney, Australia, 1998.

[10] Saqip.N,Rodrıguez.F, Diaz. P" A Compact and Efficient FPGA Implementation of the DES Algorithm", in proceeding of International Conference on Reconfigurable Computing and FPGAs, pp: 12- 18, Mexico, 2004.

[11] Swankoski. E, Brooks .R, Narayanan. V, Kandemir .M and Irwin .M, ”A Parallel Architecture for Secure FPGA Symmetric Encryption”, in Proceeding of International conference on Parallel & Distributed Processing Symposium (IPDPS), New Mexico,(2004).

[12] Aqib.A,” Efficient VLSI Implementation of DES and Triple DES Algorithm with Cipher Block Chaining concept using Verilog and FPGA”, International Journal of Computer Applications,vol(44) No(16),pp:6-15,20.