VLSI Implementation of DES & TDES Algorithm with Cipher Block Concept

Chethan Kumar K. V., S. Sujatha

***Abstract*—This paper presents FPGA implementation of the DES and Triple-DES with improved security against power analysis attacks. This is programmed in verilog. DES & TDES is basically used in various cryptographic applications and wireless protocol security layers. The proposed designs use Boolean masking, a previously introduced technique to protect smart card implementations from these attacks. Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement.DES encrypts data in 64-bit and it is a symmetric algorithm. The key length is 56-bits.**

This paper covers DES and Triple DES algorithm with Cipher Block concept, simulation results, basic FPGA technology and the implementation details of the proposed DES and Triple DES architecture. Register transfer level (RTL) of DES and Triple DES algorithm is designed, simulated and implemented separately using Verilog in different FPGA devices including Cyclone II, Spartan 3, Vertex 5 and Vertex E series FPGAs. The results from the comparison with existing implementations show that the proposed design was efficient in all aspects..

***Index Terms*— DES, FPGA, TDES, RTL, Verilog**

I. INTRODUCTION

In today's uncertain and increasingly wired world cryptology plays an important and significant role in protecting and securing communication channels, databases, and software from unwanted intruders. Modern block ciphers are widely used to grant encryption of quantities of information, and/or a cryptographic checksum to make sure the contents have not been revised. Among others the most widely used private key block cipher, is the Data Encryption Standard (DES). It was first adopted in the year 1977 by the National Bureau of Standards as Federal Information Processing Standard 46 (FIPS PUB 46) [1].DES encrypts data in 64-bit blocks using a 56-bit key. Although the original DES cipher's key size of 56 bits was sufficient and serving the purpose well when that algorithm was designed, the availability of increasing computational power made brute-force attacks feasible and predictable.

Manuscript received on May 18, 2014.

Chethan Kumar K V, He received his Bachelor of Engineering Degree from M.S Engineering College, and he is pursuing his Masters Degree from Bangalore Institute of Technology.India.

S Sujatha, Associate Professor, Dept of Electronics and Communication Engineering, Bangalore Institute of Technology, Bengaluru, Karnataka, India.

Triple DES provides a relatively simple method of increasing the key size of DES, the main feature of which is to protect against such attacks. The advantage is that there was no need to design a completely new block cipher algorithm. A much more secure version of DES called Triple-DES (TDES), which is essentially equivalent to using DES three times on plaintext with three different keys. Though it is three times slower than the original form of DES, it is comparatively more secure. DES and Triple DES implementations can be found on reconfigurable hardware using FPGA devices [3-8]. Design was successfully implemented in the cyclone II FPGA using the Altera DE1 board. The design can also be synthesized to other FPGA architectures.

II. CRYPTOGRAPHY BASICS

Cryptography describes a process of encrypting information so that its meaning is hidden and thus secured from those who do not know how to decrypt the information. It beggars description to mention the immense importance of cryptography, both in the past and in the context of today's high tech world. A cryptographic algorithm (also known as a cipher) is a step by step sequence of mathematical calculations used to encrypt and decrypt information. There are currently three different types of cryptographic algorithms: hashing algorithms, symmetric-key algorithms and asymmetric key algorithms. Hashing algorithm creates a unique fixed length signature of a block of data. Hashes are created with an algorithm, or hash function, and are used to compare sets of data. A symmetric key encryption algorithm is one that both sender and receiver within the transmission channel share the same key. The asymmetric key algorithm, also known as the public-key algorithm, uses two different keys for encryption and decryption: Public key and private key. Symmetric key encryption is performed using two methods, block cipher and stream cipher [2].

A. Block Cipher and Feistel structure

A block cipher is an encryption/decryption method in which a block of plaintext is treated as a whole and used to generate a cipher text block of equal length. Block ciphers process messages into blocks, each of which is then encrypted/ decrypted. Usually many block ciphers have a Feistel structure and this type of structure consists of a number of identical rounds of processing. In each round, a substitution is carried out on one half of the data being processed, followed by a permutation that interchanges the two halves. The original key is expanded so that a different key is used for each round.

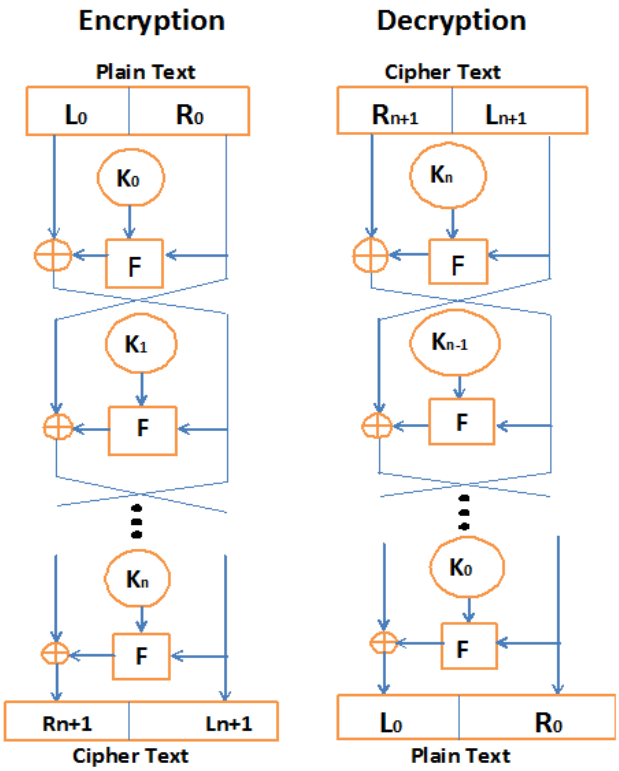

Fig.1 Feistel structure

Fig. 1 shows the general design of a Feistel cipher, a scheme used by almost all modern block ciphers. The input is broken into two equal size blocks, generally called left (L) and right (R). After that the blocks are repeatedly cycled through the algorithm At each cycle, a hash function (F) is applied to the right block and the key, and the result of the hash is XOR-ed into the left block. The blocks are then interchanged. As a result the XOR-ed result becomes the new right block and the unaltered right block becomes the left block. The process is then repeated a number of times further [12].

III. DES ALGORITHM

The Input:
T: 64 bits of clear text
k1, k2, ..., k16: 16 round keys
IP: Initial permutation
FP: Final permutation
f(): Round function
Output:
C: 64 bits of cipher text
Algorithm:
T' = IP(T), applying initial permutation
(L0, R0) = T', dividing T' into two 32-bit parts
(L1, R1) = (R0, L0 ^ f(R0, k1))
(L2, R2) = (R1, L1 ^ f(R1, k2))
.....
C' = (R16, L16), swapping the two parts
C = FP(C'), applying final permutation

A. Overall Structure

The algorithm's overall structure is shown in Fig. 3. There are 16 identical stages of processing, which are termed as rounds. There is also an initial and final permutation, known as *IP* and *FP*, which are inverses (IP "undoes" the action of FP, and vice versa). Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this criss-crossing is known as the Feistel scheme which is already been discussed in the earlier sections.

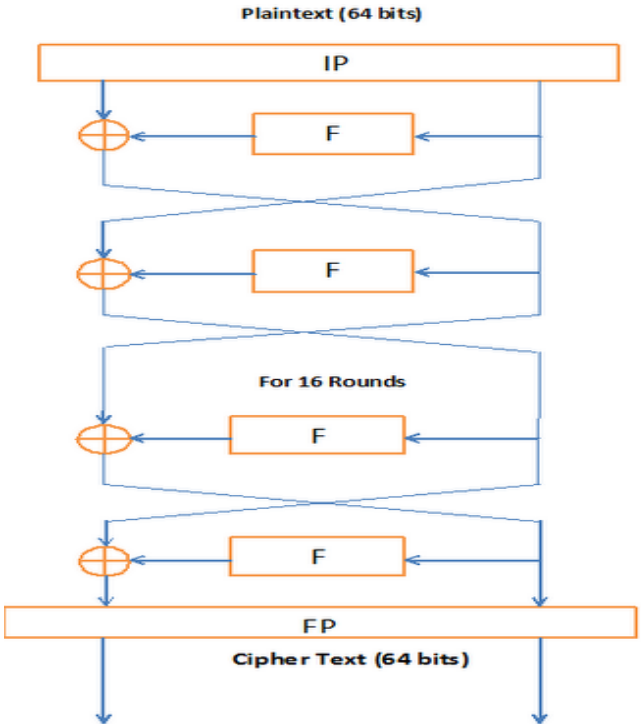

Fig.2 DES overall structure

B. DES Round Structure- the Feistel (F) function

The F-function operates on half a block (32 bits) at a time and consists of following stages:
1. Initial permutation
2. Final permutation
3. Expansion permutation (E)
4. Permutation
5. Substitution boxes (S-boxes)
6. Rotations in the key-schedule

Fig. 3 illustrates the internal structure of the DES round function F. The 32-bit half-block is expanded to 48 bits by using expansion table E that defines a permutation plus an expansion. This gives an output which consists of eight 6-bit(8*6=48bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side. The result is then XOR-ed with the subkey. 16 48-bit subkeys — one for each round — are derived from the main key using the key schedule algorithm. This 48-bit result passes through a substitution function comprising 8 S-boxes which each map 6 input bits to 4 output bits, producing a 32-bit output, which is then permuted by permutation P. This is designed in such a way that, after expansion, each S-box's output bits are spread across 6 different S boxes in the next round.

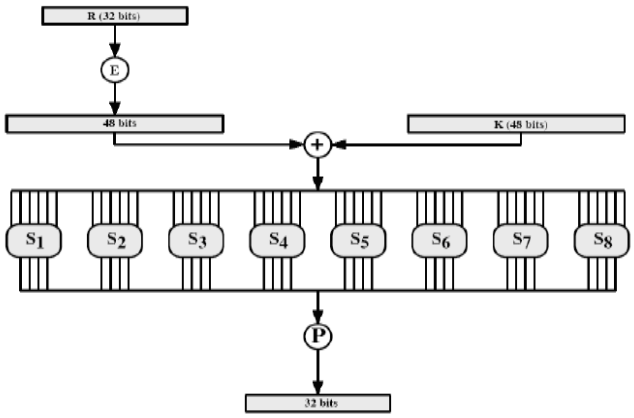

Fig.3 DES Round Structure- the F function

C. Rotations in the key-schedule

Before the round sub key is selected, each half of the key schedule state is rotated left by a number of places. This table specifies the number of places rotated. Triple DES has two attractions that assure its widespread use over the next few years[6]. First, with its 168-bit key length, it overcomes the vulnerability to brute-force attack of DES. Second, the underlying encryption algorithm in Triple DES is the same as in DES. This algorithm has been subjected to more scrutiny than any other encryption algorithm over a longer period of time, and no effective cryptanalytic attack based on the algorithm rather than brute-force has been found[5]. Accordingly, there is a high level of confidence that 3DES is very resistant to cryptanalysis. If security were the only consideration, then 3DES would be an appropriate choice for a standardized encryption algorithm for decades to come

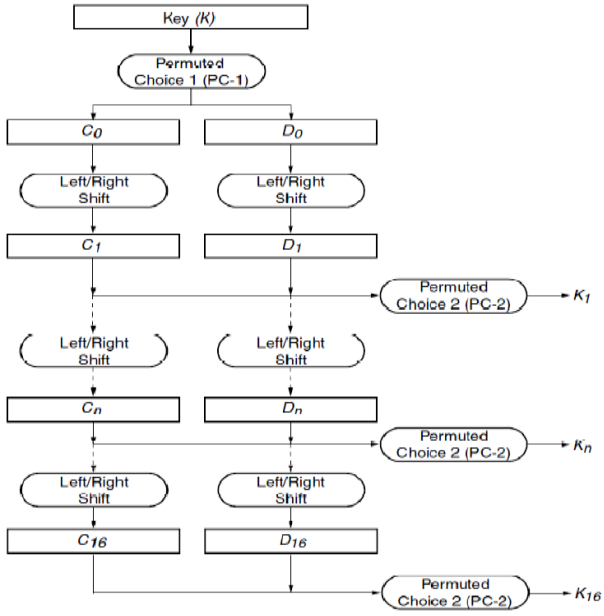

Fig.4 Key schedule calculation

D. DES Decryption Algorithm

The decryption algorithm of a block cipher should be identical to the encryption algorithm, step by step but, in a reverse order. But in case of DES cipher, the encryption algorithm is so well designed, that the decryption algorithm is identical to the encryption algorithm step by step in the same order, only with the sub keys applied in the reverse order. Feistel structure makes encryption and decryption similar processes.

E. Triple DES algorithm

The main purpose behind the development of Triple DES was to address the obvious flaws in DES without making an effort to which each map 6 input bits to 4 output bits, producing a 32-bit output, which is then permuted by permutation P. This is designed in such a way that, after expansion, each S-box's output bits are spread across 6 different S boxes in the next round. Design a whole new cryptosystem. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56), beyond the reach of brute-force techniques such as those used by the EFF DES Cracker. Triple DES has always been under some suspicion, as the original algorithm was never designed to be used in this way, however, no serious flaws have been discovered in its design, and it is today a viable and widely used cryptosystem with usage in a number of Internet protocols [9].

The standards define three keying options:

- Keying option 1: All three keys are independent. Keying option 1 is the strongest, with 3 × 56 = 168 independent key bits.
- Keying option 2: K1 and K2 are independent, and K3 = K1. Keying option 2 provides less security, with 2 × 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against meet-in-the-middle attacks.
- Keying option 3: All three keys are identical, i.e. K1 = K2 = K3. Keying option 3 is equivalent to DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST) and is not supported by ISO/IEC 18033-3 [11].

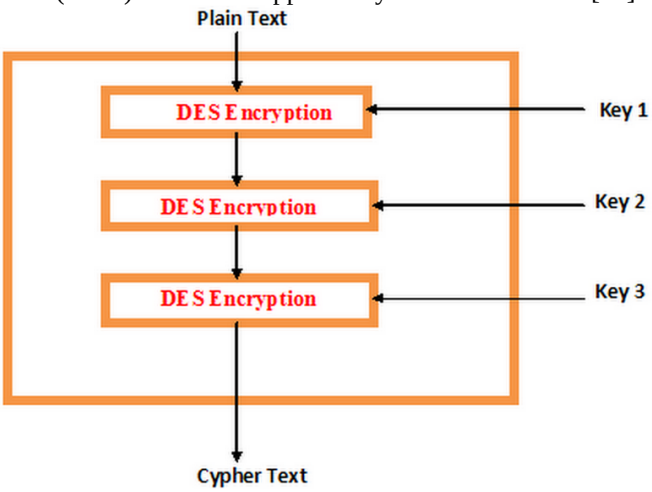

Fig.5 Working of Triple DES Algorithm

IV. IMPLEMENTATION DETAILS OF BASIC BLOCKS

A. Design Hierarchy

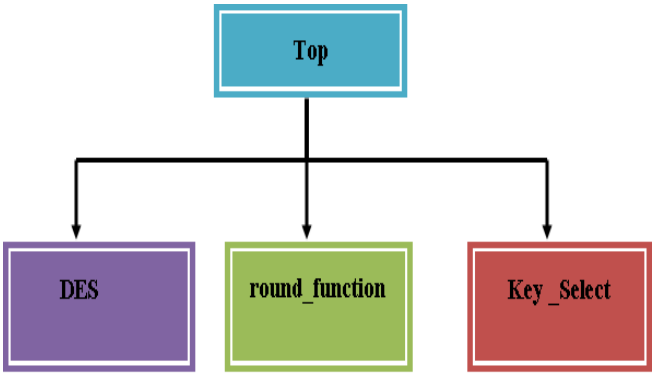

Fig.6 Design hierarchy for DES

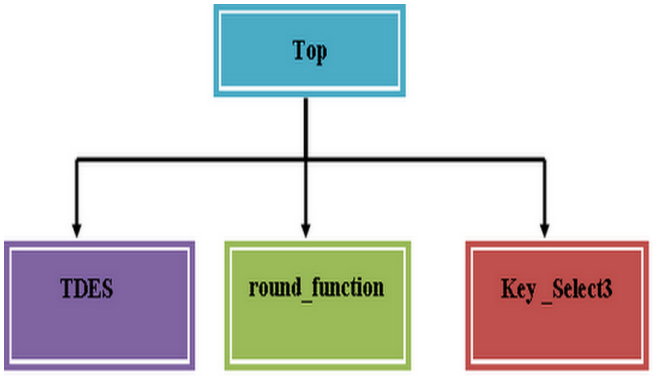

Fig.7 Design hierarchy for TDES

B. Block diagram

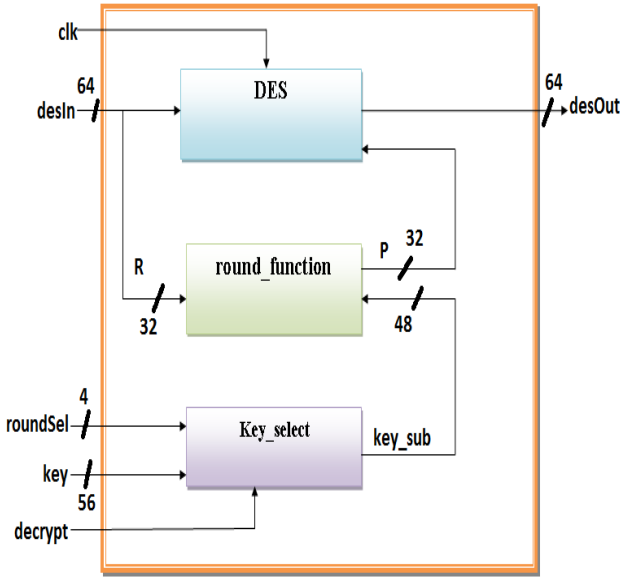

Fig.8 Block diagram for DES

C. Block description of DES

1) Round function

Applies expansion permutation and then XOR with the round key. After that applies S boxes function and returns 32-bit data. This block Implements CBC DES encryption algorithm.

2) DES

Applies initial permutation and final permutation and gives 64 bit output

3) Key select

Select one of 16 sub-keys for round, returns 48-bit data key sub

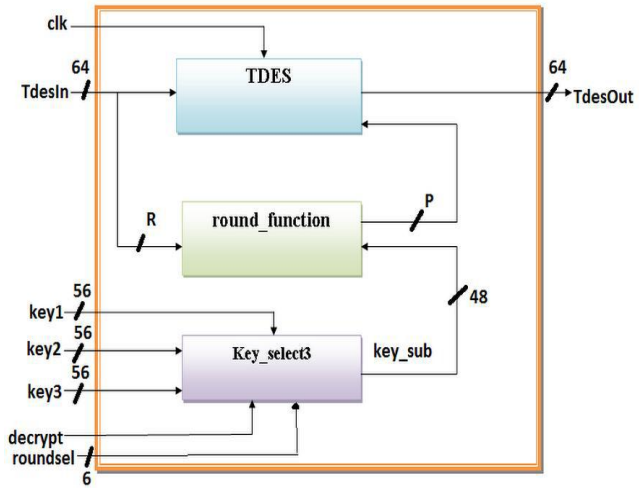

Fig.9 Block diagram for TDES

D. Block description of TDES

1) Round function

Applies expansion permutation and then XOR with the round key. After that applies S boxes function and returns 32-bit data. Implements outer triple CBC DES encryption algorithm with three keys.

2) TDES

Applies initial permutation and final permutation and gives 64 bit output.

3) Key_select3

Select three of 16 sub-keys for round, returns 48-bit data key sub.

V. EXPERIMENTAL FRAMEWORK AND RESULTS

In this section we describe the design procedure and the architecture of DES and Triple DES. Fig. 10 shows the different stages of my design. The Verilog model was synthesized with Quartus II Software targeted for Cyclone II (EP2C20F484C7) device and simulated with Modelsim. Then also the Verilog model was synthesized with Xilinx Software targeted for Spartan 3E (XC3S1600E), Vertex 5 (XC5VLX50) and Vertex E (XCV1600E) device and simulated with Modelsim. FPGA technology was chosen because it provides some important advantages over general purpose processors and application specific integrated circuits (ASICs).

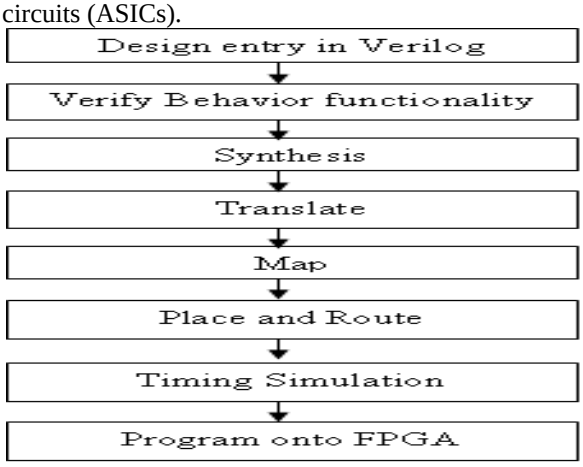

Fig.10 Implementation flow

The RTL architecture of DES and Triple DES is shown in Fig. 11 and Fig. 12 respectively.

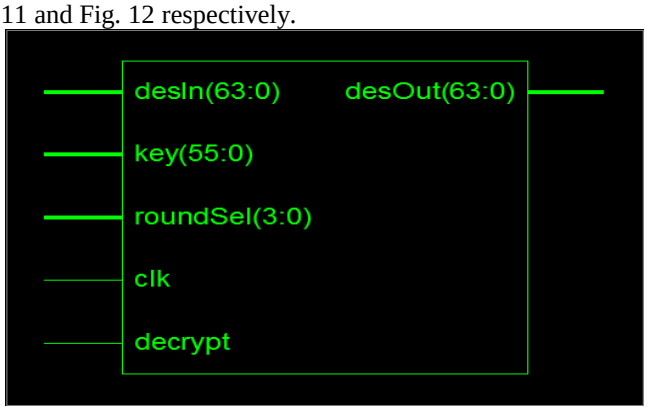

Fig.11 RTL schematic of DES

Fig.12 RTL schematic of TDES

Fig. 13 and Fig. 14 illustrate the implemented components inside the chip.

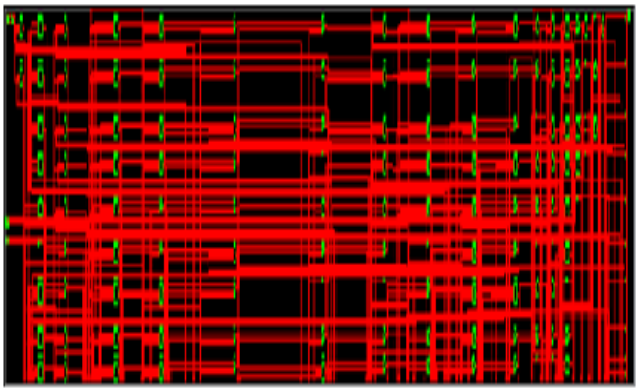

Fig.13 Technology Schematic of DES

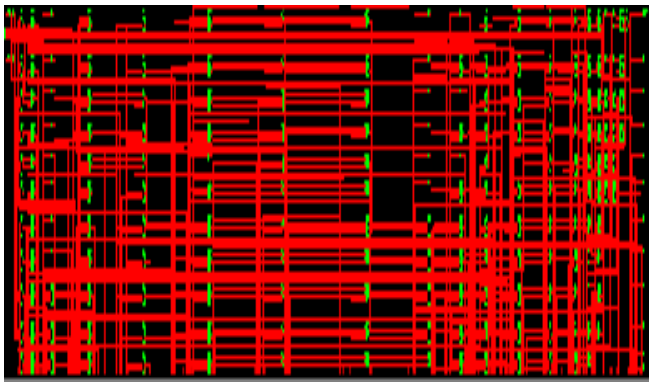

Fig.14 Technology Schematic of TDES

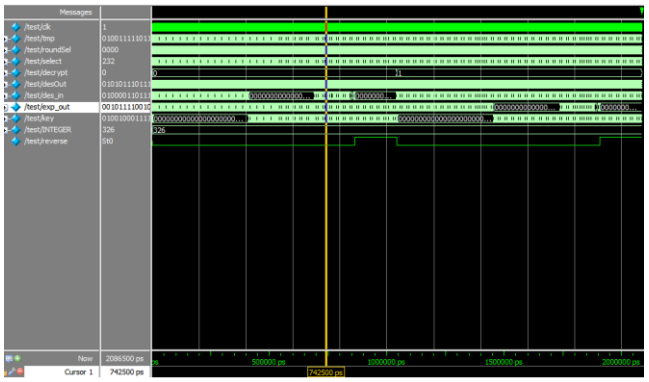

Fig.15 Output of DES

Fig.16 Output of TDES

Fig. 15 and Fig. 16 show the simulation waveform of DES and TDES algorithm. These are the sequential implementations and need 16 and 48 cycles respectively to complete a full encryption/decryption cycle

A. Table Synthesis results for DES in Vertex 5

	DES implementation	
	Vertex 5 (XC5VLX50, package ff1153,speed grade -1)	
Logic Utilization	Used	Utilization
Number of Slices	114 out of 7,200	1%
Number of Slice Flip Flops	64 out of 28,800	1%
Number of fully used LUT-FF pairs	64 out of 389	2%
Number of bonded IOBs	190 out of 560	33%
Number of BUFG/BUFGCTRLs	1 out of 32	3%

Table.1 Synthesis results for DES in Vertex 5

	TDES Existing implementation result [6]	TDES proposed implementation result
	Vertex 5 (XC5VLX50,package ff1676,speed -1)	Vertex 5 (XC5VLX50,package ff1676,speed-1)
Number of Slices	1206 / 28,800 (4%)	64/ 28,800 (1 %)
Number of Slice Flip Flops	1690 / 28,800 (5%)	887/ 28,800 (3%)
Number of fully used LUT-FF pairs	447 / 2449 (18%)	25 / 926 (2%)
Number of bonded IOBs	302 / 440 (68 %)	304 / 440 (69 %)
Number of BUFG/BUFGCTRLs	1 / 32 (3%)	1 / 32 (3%)

Table.2 Synthesis results for TDES in Vertex 5

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

It can be inferred from the above two comparisons that the proposed implementation is very much compact and efficient in all respects than others.

VI. CONCLUSION AND FUTURE WORK

A. Conclusion

In this work a compact hardware implementation of DES and Triple DES was presented. The design was implemented in real hardware with Cyclone II FPGA. The proposed architecture was also implemented with Spartan 3E, Vertex 5 and Vertex E FPGA devices and compared with the existing results. Here Cipher Block Chaining modes have been used by combining the previous cipher text block with the current message block before encrypting. DES and Triple DES algorithm are used significantly in satellite communications and electronic financial transactions, cryptographic key encryption for automated key management applications, file encryption, mail encryption, and other applications. In fact, it is extremely difficult, if not impossible, to find a cryptographic application where the DES cannot be applied. Technologies are becoming smarter and compact day by day, so we hope this work will add new dimension in that trend. This design will play a remarkable role with its significant speed and efficiency.

B. Scope and Future development

For the foreseeable future Triple DES is an excellent and reliable choice for the security needs of highly sensitive information. The AES will be at least as strong as Triple DES and probably much faster. It's the industry mandate from Visa and MasterCard that's requiring ATM deplorers' to upgrade and/or replace their legacy terminals. In a nutshell, it's all about three waves of encryption, and it's designed to make ATM transactions more secure.

REFERENCES

1. "Data encryption standard (DES)", National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, Springfield, VA, Apr. 1977.
2. T. Schaffer, A. Glaser, and P. D. Franzon, "Chip-package co-implementation of a triple DES processor," IEEE Transactions on Advanced Packaging, pp. 194-202, Feb. 2004.
3. P. Ghosal and M. Biswas, "A Compact FPGA Implementation of Triple-DES Encryption System with IP Core Generation and On-Chip Verification", International Conference on Industrial Engineering and Operations Management, 2010.
4. F. Antonios, P. Nikolaos, M. Panagiotis, and A. Emmanouel, "Hardware Implementation of Triple-DES Encryption/ Decryption Algorithm", International Conference on Telecommunications and Multimedia, 2006.
5. K. Wong, ―A single-chip FPGA implementation of the data encryption standard (des) algorithm‖ IEEE 1998 pp 827-832.
6. A. Dhir "Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs", White Paper: Spartan-II FPGAs, WP115 (v1.0) March 9, 2000.
7. C. Boyd. ―Modern Data Encryption,‖ Electronics & Communication Engineering Journal, October 1993, pp 271-278.
8. Data Encryption Standard, Federal Information Processing Standard (FIPS) 46, National Bureau of Standards, 1977.
9. Federal Information Processing Standards Publication 140-1, "Security Requirements for Cryptographic Modules", U.S. Department of Commerce/NIST, Springfield, VA: NIST, 1994.
10. D. C. Feldmeier, P. R. Karn, "UNIX Password Security – Ten Years Later," CRYPTO'89, Santa Barbara, California, USA, pp. 44-63, 1989.
11. NIST Special Publications 800-20, "Modes of Operation Validation System for the Triple Data Encryption Algorithm", National Institute of Standard and Technology, 2000.
12. C. Boyd. ―Modern Data Encryption,‖ Electronics & Communication Engineering Journal, October 1993, pp 271-278.
13. W. Diffie, ―Cryptographic Technology: Fifteen Year Forecast‖ Reprinted by permission AAAS, 1982 from Secure Communications and Asymmetric Crypto Systems. AAAS Selecte8 Symposia. Editor: C.J. Simmons. Vol. 69, Westview Press, Boulder, Colorado, pp 38-57.