International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Implementation of Triple Data Encryption Standard Architecture

A. Ram Kumar[1], Shaik Mubeena[2], V. Surendra Babu[3]

[1]Assistant Professor Sir C. R. Reddy College of Engineering, Eluru, Andhra Pradesh, India
[2] PG scholar, Sir C. R. Reddy College of Engineering, Eluru, Andhra Pradesh, India
[3]Assistant Professor Department of ECE, Sir C. R. Reddy College of Engineering, Eluru, Andhra Pradesh, India

ABSTRACT

Cryptography plays very important role in security of data. Cryptography means to transfer sensitive information across insecure networks like internet so that it cannot be read by anyone except the person whom we want to send it. It basically hides the information. The federal organization used the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA), which may be used to protect sensitive data. Cryptography algorithms are divided into Symmetric and Asymmetric key cryptography. Symmetric Cryptography is further divided into Block ciphers and Stream Ciphers. This paper discusses Implementation of Triple Data Encryption Standard Architecture of different block cipher algorithms of Symmetric Key Cryptography. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. The proposed architecture is modeled in the VHDL design language and simulation results with the help of Xilinx software tool.

Keywords: DES, Triple-DES, Encryption/Decryption.

I. INTRODUCTION

When we talk about security, it is necessary that we know cryptography. Today it is must to secure sensitive data transmitted over network or kept in storage from attackers. 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.

The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted by National Bureau of Standards. For DES, data are encrypted in 64-bits blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.

Recently, and mainly because of the increased speed of computing systems, DES has come under brute force attack on several occasions demonstrating its vulnerability to exhaustive searching of the key space. Triple-DES is simply the DES algorithm applied three times using either two or three keys. 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.

The paper is organized as follows: In sections 2 and 3 the DES and Triple DES Block Cipher is described briefly. The proposed TDES architectures are presented in details in section 4. The simulation results implementation is shown in section 5, and the paper conclusions are given in section 6.

II. EXISTING DATA ENCRYPTION STANDARD ALGORITHM

The Data Encryption standard is used to protect electronic data. DES algorithm uses symmetric block cipher for encrypting and decrypting data. Encryption converts data into gibberish language called cipher text. Decrypting the cipher text gives us back the original data that is plaintext. Converting the information from ciphertext to plaintext, we use a standard form of algorithm called Symmetric algorithm.

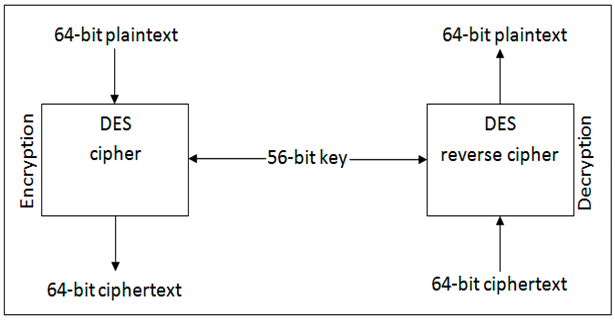

Figure 1. Encryption and Decryption with DES

DES takes an input of 64-bits and the output is also of the same size. As shown in above figure 1, The process requires a second input, which is a secret key with length of 64-bits, every eighth bit is used as parity checking bit. Therefore, 56-bits take part in the algorithm to encrypt data. Block cipher algorithm is used where message is divided into blocks of bits. Block cipher is used for encryption and decryption. These blocks of bits are put through substitution, permutation, and other different mathematical functions.

III. PROPOSED TRIPLE DES ALGORITHM

Triple-DES cipher was created because DES algorithm, Invented in the early 1970s using 56-bit key. The effective security, which Triple-DES provides, is 168-bits, when an attacker uses meet in the middle attacks.
Triple-DES works in much the same way as DES, except that goes through three cycles during the encryption process, using three keys: encryption, decryption, and another encryption. It has a key length of 192-bits (64-bits x 3 keys), but its actual strength is 168-bits (56-bits x 3 keys). This method is three times as strong as DES, yet it also means that it is three times slower because of the triple processing. Due to key length the Triple-DES is more defined then the DES algorithm & also used in many applications. The block diagram of TDES is shown below Figure 2. Triple-DES uses DES three times for encryption likewise for decryption. The work is using three block of DES to perform operation of Triple-DES.

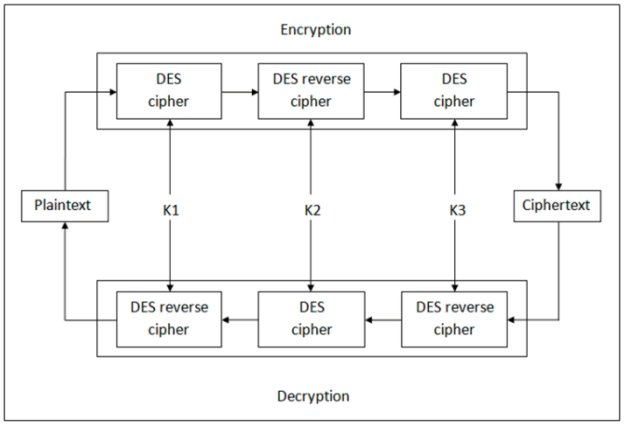

Figure 2. Triple DES Block Diagram

Triple-DES Encryption and Decryption process is as follows:

1) Encrypt using first key and plaintext to produce first ciphertext.
2) Decrypt using first ciphertext and second key to produce second ciphertext.
3) Encrypt using second ciphertext and third key to produce final ciphertext.
4) The output is produce final ciphertext.
5) Decryption of a ciphertext is a reverse process.

First decrypt using third key, then encrypt with second key, and finally decrypt with first key.

IV. ARCHITECTURE FOR THE TRIPLE DES ALGORITHM

4.1. Encryption

Triple DES provides a relatively simple method of increasing the key size of DES. In Figure 3, the proposed Triple-DES architecture is presented. It consists of 16 rounds of DES function. Here, the data path of this architecture consists of a key scheduling, round function, initial permutation, and final permutation.

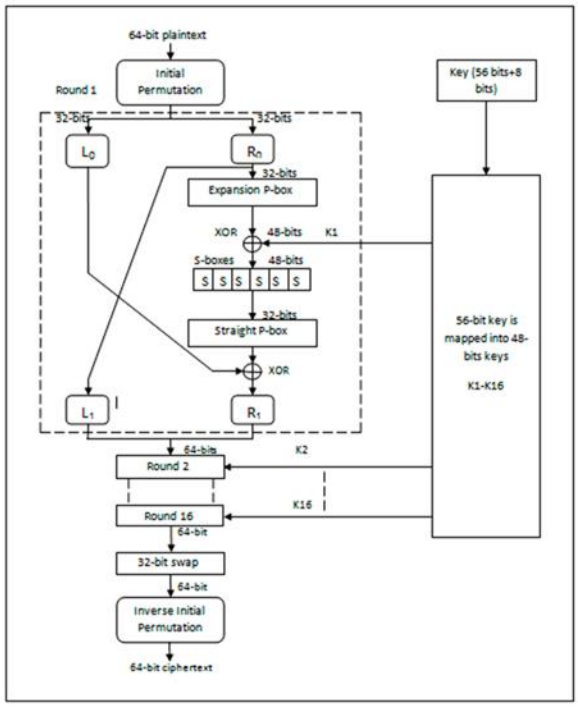

Figure 3. Triple-DES Algorithm

DES operates on a 64-bit block of plaintext. After an initial permutation the block is broken into a right half (R0) and left half (L0), each 32-bits long. Then there are 16 rounds of identical operations, called function F, in which the data are combined with the key. After the sixteenth round, the right and left halves are joined, and a final permutation (the inverse of the initial permutation) finishes off the algorithm.

4.1.1. Key Schedule

As per the DES algorithm needs, the architecture shown in Figure 3 requires a round key generation in each rounds. The steps for the round key generation process are shown in Figure 4. The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher keys for the each individual rounds.

In the DES algorithm, sixteen rounds are required to generate the sixteen round keys. The input key has 64 bits. However, each eighth bit is used as parity checking bit. The 56-bit input key is provided to the Permutation Choice 1 (PC-1). The permutation choice-1 block permutes the 56-bit input key is then created as two 28-bit quantities, labeled C0 and D0. After C0 and D0 are connected to Cn and Dn of the next round. Out of 16 rounds of operation, 12 rounds have 2 left circular shifts and the rest 4 have only 1 (specified for each round), and then 48 sub-key bits are selected by Permuted Choice 2 (PC-2), 24-bits from the left half, and 24-bits from the right half. The 56 bits produced after circular shifts goes into the second round of key generation to produce the second round key and so on producing 16 keys in total in the whole process as shown in Figure 4. The round key generation for decryption is similar, only the sub-keys are in reverse order as compared to encryption.

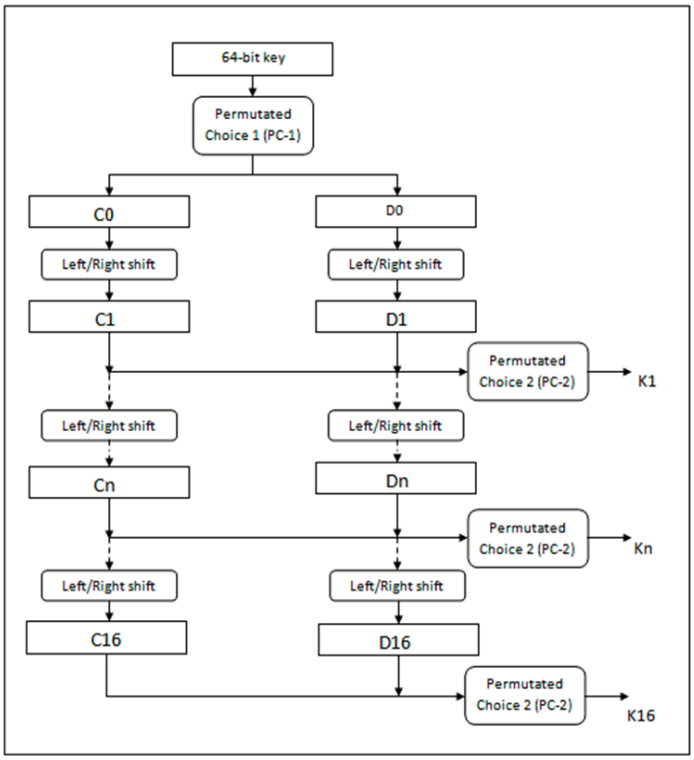

Figure 4. Key Schedule Calculation

4.1.2. Rounds function

The algorithmic implementation of DES is known as DEA for Data Encryption Algorithm. DES uses 16 rounds. Each round of DES is a feistel cipher, as shown in Figure 3. The round block divides its input into two equal parts, the data bits have parts L0 of 32-bits and R0 of 32-bits. Similarly, key bits are divided in two parts C0 and D0 each of 28-bits of length. The 56-bits are used to generate the 48-bit round key through the

permutation choice 2. As shown in below Figure 5. The 32-bit round key R0 is expanded to 48-bit round key through expansion permutation. The output from PC2 block is XOR with expansion permutation block to get the 48-bit address for the substitution box (S-box). The 48-bits is given as sequence to S-box into 8 blocks, each of 6-bits. The S-box replaces every 6-bit of data to 4-bit data.

$$Ln = Rn-1 \; Rn = Ln-1 + F(Rn-1, Kn)$$

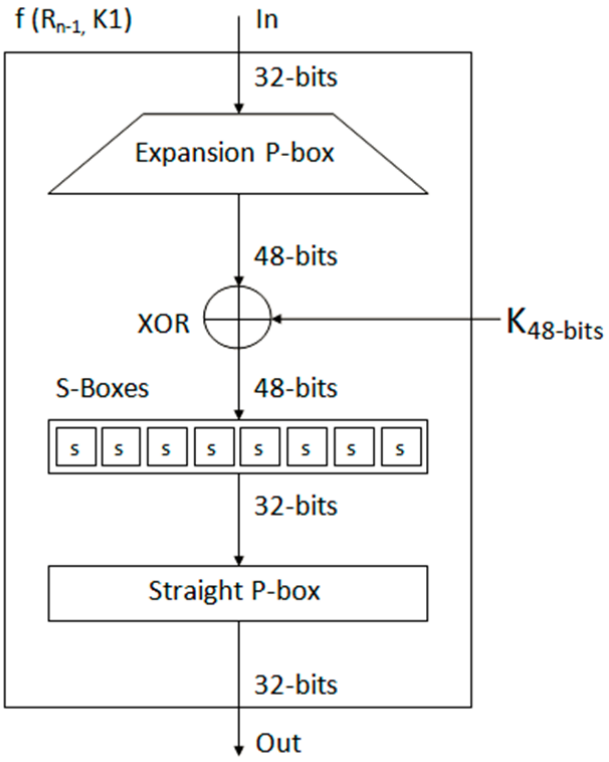

Figure 5. DES function

4.1.3. Substitution Boxes (S-Boxes)

As shown in below Figure 6, the R input is 32-bits. This R input is first expanded to 48-bits by Expansion/Permutation. The resulting 48-bits are XORed with Kn. This 48-bit result is divided into eight 6-bit inputs and each 6-bit input fed into a separate S-box. Each S-box produces a 4-bit output. Therefore, the eight S-boxes together generate a 32-bit output. As you can see, the overall substitution step takes the 48-bit input back to a 32-bit output.

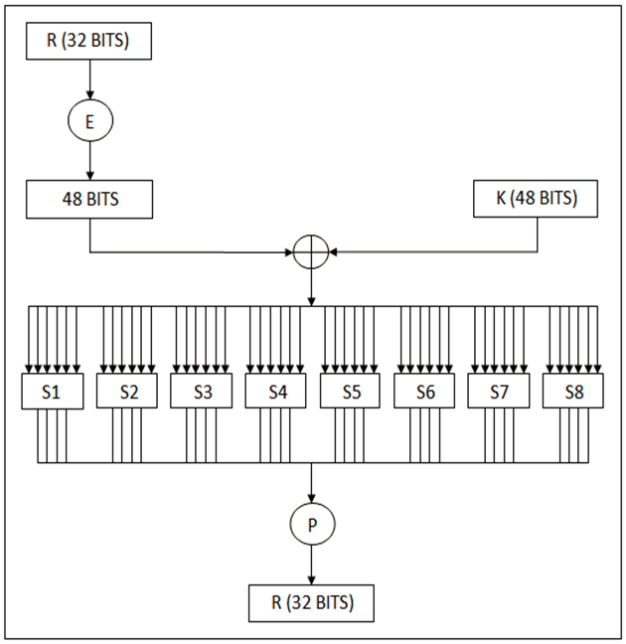

Figure 6. Calculation of f(R, k)

4.1.4. Permutation

32-bits are permuted according to a given array of permuted choice 2. After permutation, 32-bits are XORed with L0. Result is become Right side (R1) for next round, while old R0 becomes new Left side (L1). This process is repeated for sixteen rounds using the keys (K1……K16). After round 16, R16 and L16 are concatenated and then final permutation is done. Now result is 64-bits cipher text.

4.2. Decryption

Decryption uses the same algorithm as encryption, with the only difference that the round keys are used in the reverse order (K16…….K1).

V. SIMULATION RESULTS

Both Data Encryption Standard (DES) and Triple Data Encryption Standard (TDES) are compared in this section. Simulation wave forms of Data Encryption Standard (DES) and Triple Data Encryption Standard (TDES) Encryption and Decryption are separately illustrated in following, figures.

5.1. DES Encryption and Decryption results

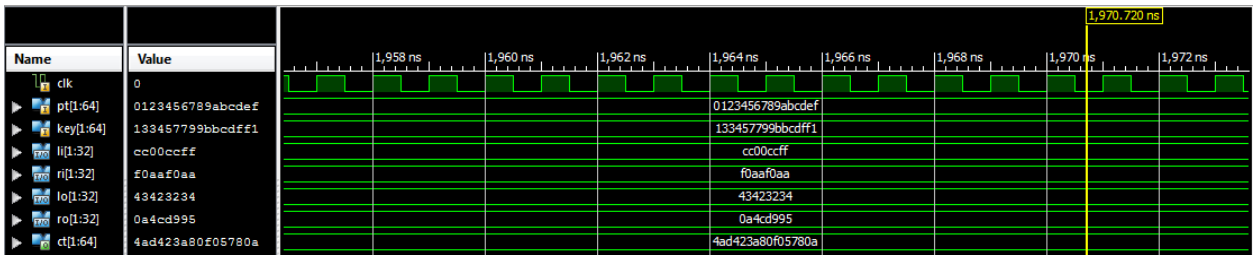

Figure 7. Waveform of DES Encryption Simulation

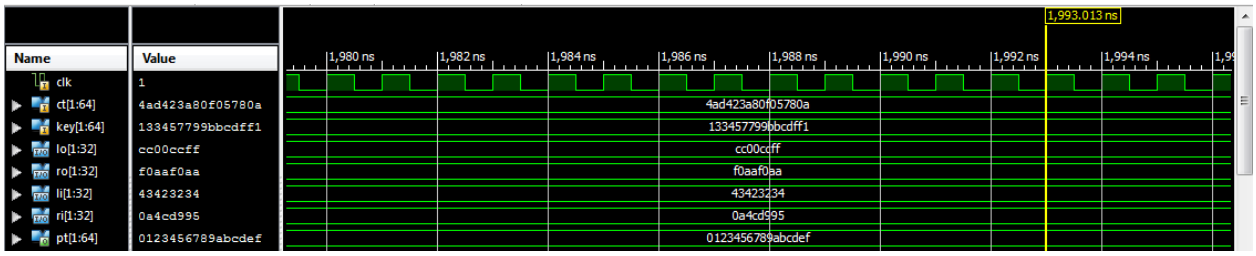

Figure 8. Waveform of DES Decryption Simulation

5.2. Proposed Triple-DES Encryption and Decryption results

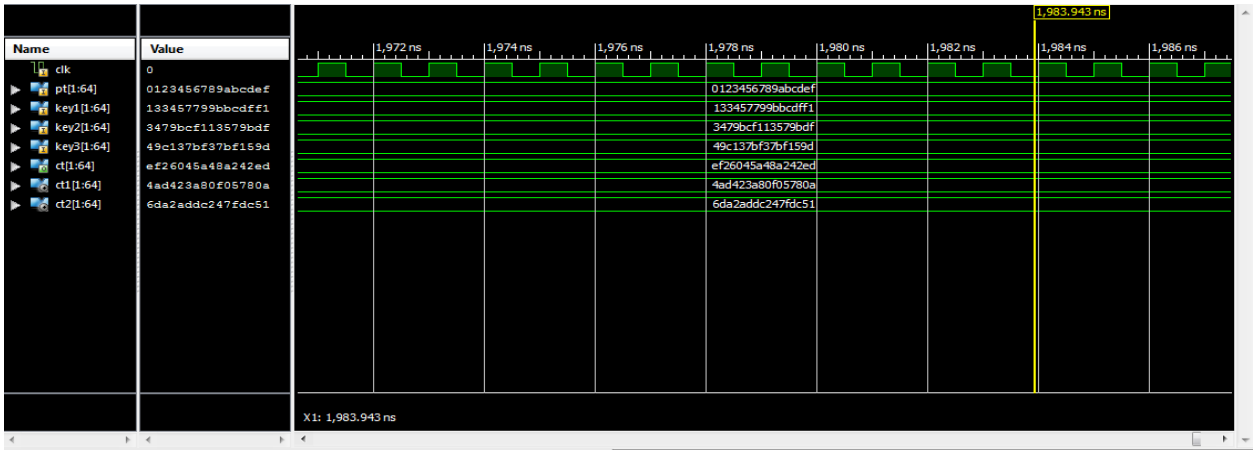

Figure 9. Waveform of Triple-DES Encryption Simulation

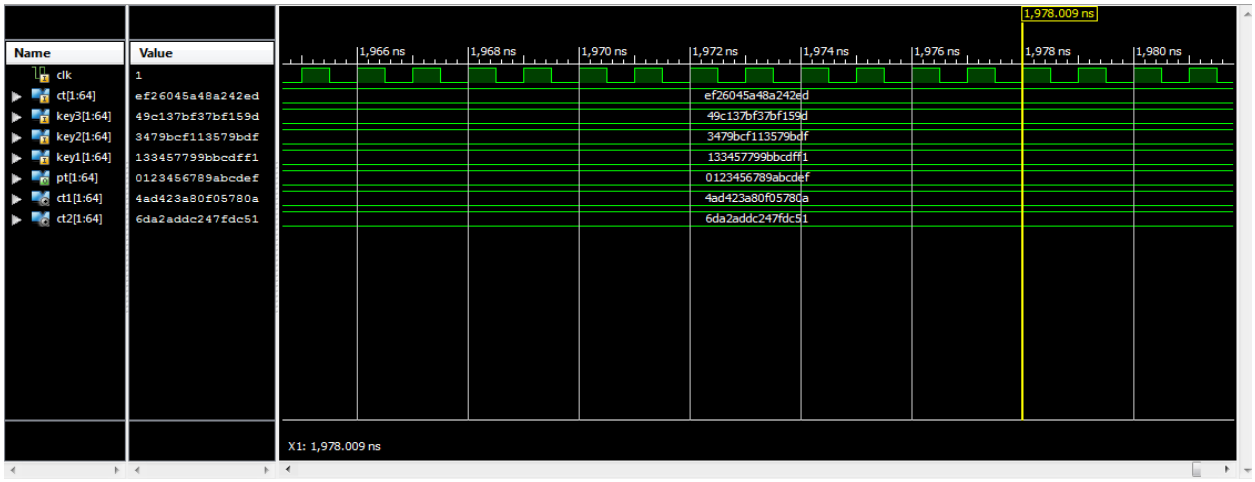

Figure 10. Waveform of Triple-DES Decryption Simulation

The evaluation results of the architectures proposed are presented and compared with previous architectures using Xilinx, vertex 5. The comparison of the proposed design with the existing one is shown in the table 1.

Table 1. Comparison of existing DES and proposed TDES

Factors	Existing DES	Proposed TDES
Key Length	56 bits	168 bits
Block Size	64 bits	64 bits
Rounds	16	48
Keys	Single key	Different three keys
Cipher type	Symmetric block cipher	Symmetric block cipher
Algorithm Structure	Fiestel Network	Fiestel Network

The comparison of the results of the existing and proposed architectures using Xilinx vertex 5 is given below in table 2 and table 3.

Table 2. Timing Report of DES and TDES

Parameter	Existing DES	Proposed TDES
Minimum Period	2.678ns	3.066ns
Maximum Frequency	373.420MHZ	326.131MHZ
Minimum Input Arrival Time before Clock	3.309ns	3.482ns
Maximum Output Required Time after Clock	4.525ns	6.558ns

Table 3. Comparison of results of the existing and proposed architectures

Factors	Existing DES	Proposed Triple-DES
Number of Slices	5%	21%
Number of Slice Register	1%	3%
Number of Slice LUTs	3%	12%
Number of Slice LUT-Flip Flop pairs	3%	12%
Number of bonded IOBs	28%	46%
Number of BUFGs	3%	3%
Delay	5.008ns	6.942ns
Throughput (Gbps)	1.306	1.141
Throughput (Mbits/s)	1306	1141
Throughput/Area (Mbps/slices)	2.027	0.472

VI. CONCLUSION

The concept of cryptography long with encryption and decryption is explained. DES has 16 rounds of operation. The plaintext is taken to 16 rounds of operation, which produces a cipher text (final output). With Triple DES, it will encryption and decryption the block and a completely different output is generated with a final combination. It is said that the security is 192-bits encryption/decryption, but also argued that regardless of the keys, the security is only 168-bit. It is a safe but that Triple-DES is exponentially stronger than the previous DES.

IV. REFERENCES

[1]. Data Encryption Standard, Federal Information Processing Standard(FIPS)46, National Bureau of Standards, 1977.

[2]. Applied Cryptography : Protocols, Algorithms, and Source Code in C, by Bruce Schneier.

[3]. Understanding Cryptography:A Textbook for students and Practitioners by christof Paar, Jan Pelzl, Bart Preneel.

[4]. Coppersmith, Don. "The Data Encryption Standard(DES)and its strength against attacks." IBM journal of research and development 38.3(1994):243-250.

[5]. Luminita Scripcariu "A Study Of Method Used To Improve Encryption Algorithms Robustness" Published On IEEE in July 2015.
[6]. Mohammed M. Alani "DES96 – improved DES Security" Published On IEEE in June 2010.
[7]. V. Pasham et.al, "High - Speed DES and Triple DES Encryption/ Decryption", XAPP270(v1.0)August 03, 2001.
[8]. Amit Dhir, "Data Encryption using DES/Triple-DES Functionality in Sparatan-2 FPGAs", WP115(v1.0), 9 March, 2000.