Performance Analysis of 64-BIT Data Encryption Standard Using VHDL

Manpreet Kaur, Parminder Singh Jassal,

Abstract— **There are many encryption algorithms that are now commonly used in computation, but the U.S. government has adopted the Data Encryption Standard DES /TDES to be used by Federal Information Processing Standard (FIPS) 1996 departments and agencies for protecting sensitive information. As the TDES has been widely adopted for various applications such as: credit card details, banking transaction, e-commerce. The various DES/TDES hardware architectures implements to meet different requirements i.e. security. Typical examples are high operating frequency design and low area design. Due to the importance of the DES/TDES algorithm and the numerous applications that it has, our main concern DES/TDES Encryption/Decryption using three keys and implement on the device which occupy lowest area and give higher operating frequency. The low-cost implementation and moderate throughput practically suitable for security focused low resource applications. The design is simulated and synthesize in Xilinx ISE 13.2 with family Virtex-7 (XC7VX330t– 3ffg1157). The verified model synthesized DES which utilized (1968) slices, LUTs (1808), operating frequency (593.578 MHz) and throughput (2374.312Mbits/s)* corresponding to [1], [15], respectively and TDES synthesized to which utilized 1200 slices, LUTs (1478), operating frequency (339.474 MHz) and Throughput (1357.896 Mbits/s)* [15] . The former DES/TDES algorithm emphasizes its operating frequency and throughput using Virtex-2. Its biggest disadvantage use large area and gives lower operating frequency. Generally, the embedded applications do not require very fast speed. Our work provides lowest area, high operating frequency (132.474 MHz) and throughput (529.896 Mbits/s) of TDES.**

Index Terms— **Cryptography, DES, TDES, Encryption, Decryption, Implementation results.**

I. INTRODUCTION

The internet is a global system of interconnected computer networks. As demand and the importance of exchanging valuable data over the internet is booming. The main demand for today is to protect valuable data from unauthorized access. As the applications that is increasing day-by-day the requirement of network security to providing quality of service. The security is most challenging aspects in the internet. Cryptography is the one of main categories for computer security that converts the original and readable data to unreadable form. Encryption is best solution to ensure security. Many encryption algorithms are used in information security system. In this thesis tries to fair comparison between most common and basic symmetric key cryptography algorithms: Data Encryption Standard (DES) and Triple Data Encryption Standard (TDES). The main concerns are the different settings of these algorithms based on these parameters: frequency, area and throughput in present work.

In [1], DES, AES and Blowfish are analyzed based upon these parameters execution time, memory required for implementation and throughput. It concluded that the Blowfish algorithm is best performed as compared to DES and AES algorithms. TDES algorithm is not implemented in this paper.

In [13], this paper presented reconfigurable hardware implementation of the Data Encryption Standard (DES) algorithm using VirtexE XCV400e device. It concluded DES round design achieved a data encryption/decryption rate of 274 Mbits/s occupied 117 CLB slices. There is no focus on maximum operating frequency and throughput.

DES and TDES [15] are implemented in virtex-2 devices for performance evaluation based on area used for slices, LUTs and maximum clock rate. It concluded that are required for slices and LUTs is less for DES compared to TDES, this design can run at over 237 MHZ making it the fastest DES encryptor. There is no focus on maximum clock rate, throughput and less area use for these algorithms.

This paper is organized as follows: the second section presents the DES and TDES algorithms under study. The third section gives the encryption/decryption simulation results of DES and TDES algorithms. The comparison results and relevant conclusions are drawn briefly in section 4.

II. DES AND TDES ALGORITHM

A. *DES (Data Encryption Standard)-*

DES algorithm is designed to encipher and decipher 64 bits blocks of data by using of a 64-bit key. It maps 64-bit input block into a 64-bit output block. Actually it uses 56-bit key, because one bit in each of 8 octets is used for odd parity on each octet [7]. The basic operation of DES can be understood with the help of figure (2.1). The same 56-bit cipher key is used for encryption and decryption. There are three operations performed in DES algorithm: - Encryption, Decryption and Key Generation [1].

Manpreet Kaur, M-Tech Student, Department of Electronics, Yadvindra College Of Engineering, Talwandi Sabo (Pb)- INDIA

Parminder Singh Jassal, Assistant Professor, Department of Electronics, Yadvindra College Of Engineering, Talwandi Sabo (Pb)- INDIA

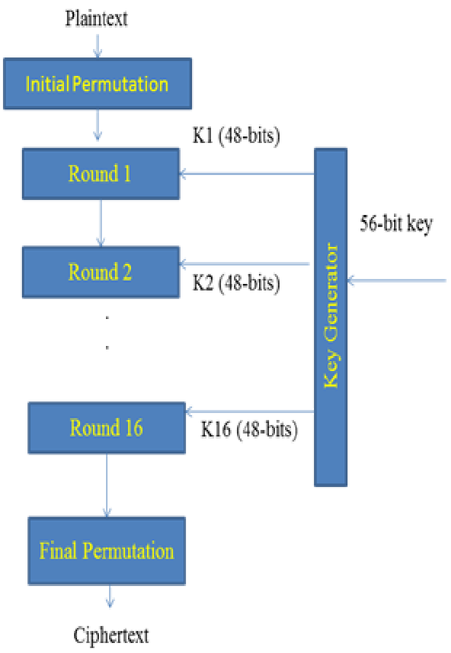

Fig.1- General Structure of DES [1]

Algorithm Encryption Steps

Step 1: Initially get 64-bit key and plaintext to be encrypted.

Step 2: Perform initial permutation on plaintext.

Step 3: Then divide the plaintext into two 32-bit parts.

Step 4: The key generator generates round key which perform 16 times round function.

Step 5: Finally, use the output of 4 steps to perform final permutation (fp) in the form of original ciphertext.

Algorithm Decryption Steps

Decryption process performs all the sane steps of Encryption process but in reverse order

Algorithm Key Generator Steps

Step 1: Initially get the 64-bit key.

Step 2: Then perform parity bit drop to reduce it to 56-bits.

Step 3: Divide it into two equal 28-bits parts.

Step 4: According to round function it perform shift left operation of the 28-bit data.

Step 5: Perform the compressed permutation use the output of step 4.

Step 6: Repeat the step 4 and step 5 to produce 16 round keys

B. *TDES (Triple Data Encryption Standard)-*

The 3DES is more secure version of DES [16]. It is an enhancement of DES. The encryption standard of 3DES was proposed based on the existing basic algorithm DES. The TDES algorithm can use two or three 56-bit key. So the effective length of key is up to 168-bits.The encryption\decryption operation of TDES is a operation of DES encryption\decryption operation (as specified in ANSI X9.52). 3DES is defined by following function in figure (2.5) [15].

$C = DES_{k3}\ \{DES_{-1}$

$_{k2}\ \{DES_{k1}\ (P)\}$

Where P = Plaintext

C = Ciphertext

$DES_{\ k}$ = DES encryption using K

DES_{-1}

$_{k}$ = DES decryption using K

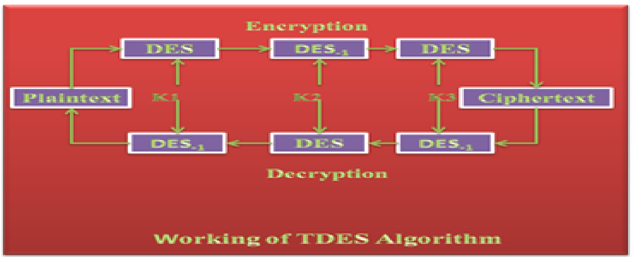

Fig 2:-Working of Algorithm [15]

III. Simulation Result

Encryption Simulation Waveform of DES Encryption is shown in Fig 3. The input key, data input & Encrypted output shown below:

Key [55:0]:- "aaaaaaaaaaaaaa".

Plaintext – desIn [63:0]:- "bbbbbbbbbbbbbbbb".

Encryption result is:

Encrypted output- desout [63:0]:- "ac182599db161651".

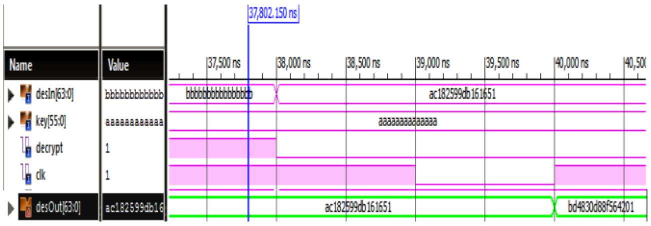

Fig 3:- Waveform of DES Encryption Simulation

Decryption Simulation Waveform of DES Encryption is shown in Fig 4. The input key, data input & Decrypted output shown below:

Key [55:0]:- "aaaaaaaaaaaaaa".

Ciphertext – desIn [63:0]:- "ac182599db161651".

Decryption result is:

Decrypted output- desout [63:0]:- "bbbbbbbbbbbbbbbb".

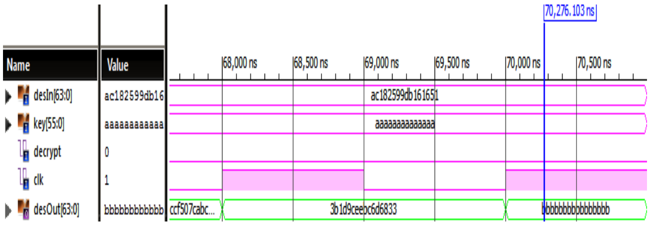

Fig 4:- Waveform of DES Decryption Simulation.

Encryption Simulation Waveform verifies TDES Encryption for following Key and Plain text values:

This Encryption Simulation Waveform verifies TDES Encryption for following Key and Plain text values:

Key1 [55:0] - x "00000000000000000000000000000000000000000000000000000"

Key2 [55:0] - x "00000000000000000000000000000000000000000000000000000"

Key3 [55:0] - x "00000000000000000000000000000000000000000000000000000"

Plain Text input: x "95f8a5e5dd31d900"

The encrypted result is:

Encrypted output: x "8000000000000000"

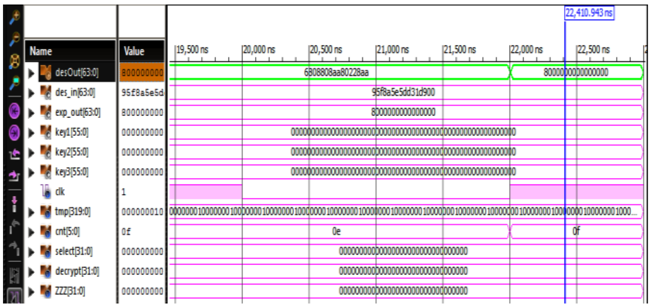

Fig 5- TDES Encryption Simulation Waveform

This Decryption Simulation Waveform verifies TDES Decryption for following Key and ciphertext input values:
Key1 [55:0] - x
“00000000000000000000000000000000000000000000000000000”
Key2 [55:0] - x
“00000000000000000000000000000000000000000000000000000”
Key3 [55:0] - x
“00000000000000000000000000000000000000000000000000000”
Ciphertext input: x “8000000000000000”
The decrypted result is:
Decrypted values: x “95f8a5e5dd31d900”

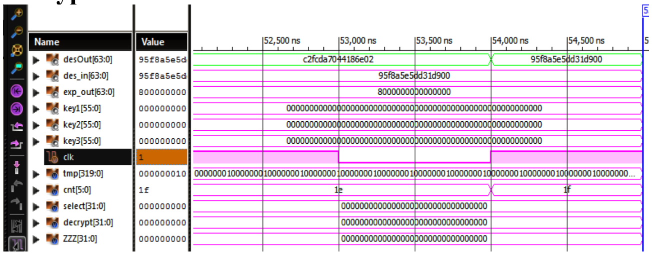

Fig 6- TDES Decryption Simulation Waveform

This Encryption Simulation Waveform verifies TDES Encryption for following Key and Plain text values:
Key1 [55:0] - x
“00000000000000000000000000000000000000000000000000000”
Key2 [55:0] - x
“00000000000000000000000000000000000000000000000000000”
Key3 [55:0] - x
“00000000000000000000000000000000000000000000000000000”
Plain Text input: x “95f8a5e5dd31d900”
The encrypted result is:
Encrypted output: x “8000000000000000”

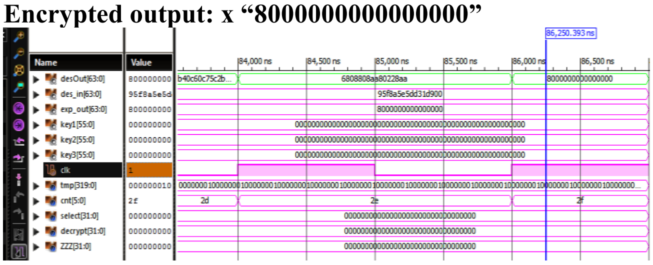

Fig 7- TDES Encryption Simulation Waveform

IV. Experimental Results and Conclusion

The design is simulated and synthesize in Xilinx ISE 13.2 with family Virtex-7 (XC7VX330t – 3ffg1157).the verified model is synthesized to get an estimate of number of slices, LUTs, operating frequency and throughput.

A. DES Implementation Result

In this work DES is analyzed on Virtex -7 (XC7VX330t – 3ffg1157) device. The table 1. depicts that the former DES algorithm emphasizes its operating frequency and throughput ,large area are biggest disadvantages.

Table1. DES Implementation Results

Author	Slices	LUTs	Max. Frequency (MHz)	Through-put (Mbits/s)
Nazar A.Saqib et.al[13]	117	-	68.05	274
V.Pasham et.al [15]	5185	5036	237	948
A.Ramesh et.al [1]	-	-	0.0025	0.01015012
This Work	1968 (0%)	1808 (0%)	593.578	2374.312

B. TDES Implementation Result

As shown in table2. the former TDES algorithm emphasizes its operating frequency and throughput using Virtex-2. Its biggest disadvantage use large area and gives lower operating frequency. Generally, the embedded applications do not require very fast speed. So, our TDES encryption is based FPGA design using Virtex-7 device. Our work provides lowest area, high operating frequency and throughput.

Table2. TDES Implementation Results

Author	Slices	LUTs	Max. Frequency (MHz)	Throughput (Mbits/s)
V.Pasham et.al [15]	(54%)	(56%)	207	828
This Work	1200 (0%)	1478 (0%)	339.474	1357.896

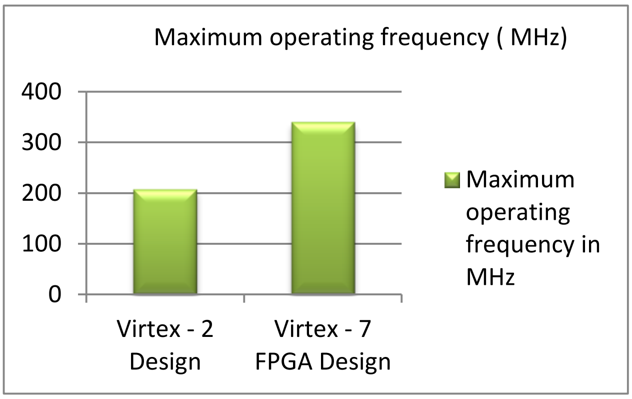

Fig 8- Comparison graph of TDES (Max. operating frequency) .

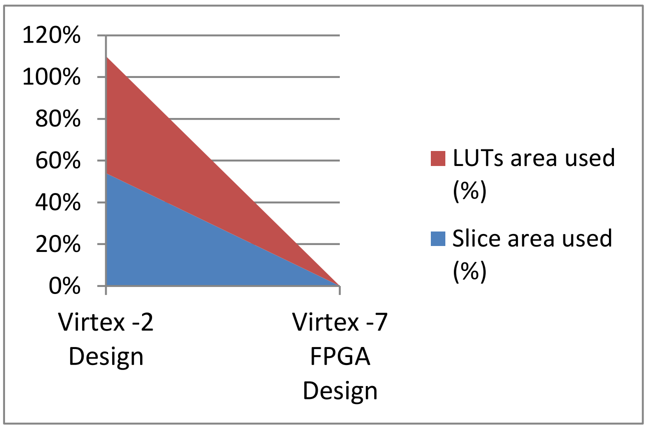

Fig 9- Comparison graph of TDES (Area)

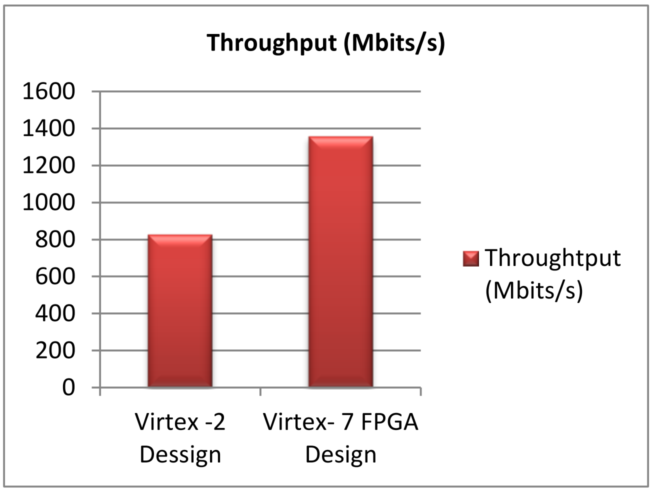

Fig 10 – Comparsion graph of TDES (Throughtput).

V. Conclusion

In this thesis work, an efficient and compact performance analysis of DES algorithm. VLSI or FPGA implementations achieve ultra high throughputs depending on the design strategy; design resources and optimization work both at algorithm and design level. As shown in Table 1 and 2 the frequency and throughput of DES and TDES is higher than previous work, the number of slice and LUTs area used is very less as compared to previous work.

VI. Future Scope

With the development of Algorithms, FPGA based Algorithms have become much smaller in occupy area like Slice used area or LUTs used area and are capable of operating much faster than ever before. So Algorithms that consume less area and high operating frequency are required. The pipelined implementation of DES and TDES can be used to reduce the area and to improve operating frequency for future work.

References

[1] A. Ramesh et.al, "Performance Analysis of Encryption Algorithms for Information security", IEEE Department of computer science and engineering," M.S University 2013.

[2] Md Imran Alam et.al, "Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, ISSN: 2277 128X, October 2013.

[3] Akash Kumar Mandal et.al, "Performance Evaluation of Cryptographic Algorithms DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012.

[4] Shraddha Soni et.al, "Analysis and Comparison between AES and DES Cryptographic algorithm", International Journal of Engineering and Innovative Technology, Vol. 2, Issue 6, December 2012.

[5] O P Verma et.al, "Performance Analysis of Data Encryption Algorithms", IEEE International Journal of Computer Applications, Vo1.42, No.16, March 2011.

[6] Jawahar Thakur et.al, " DES, AES and Blowfish : Symmetric Key cryptography Algorithm Simulation Based Performance Analysis," International Journal of Emerging and Advanced Engineering , ISSN 2250-2459, Vol. 1, Issue 2, December 2011.

[7] Nagesh Kumar et.al, "Performance Analysis of Symmetric Key Cryptography Algorithms: DES, AES and Blowfish" International Journal of Engineering Sciences ISSN: 2229-6913, Issue September, Vol.4, 2011.

[8] Simar Preet Singh et.al, "Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication, Vol. 2, No. 1, pp. 125-127, January-June 2011.

[9] Saeid Taherkhani et.al, "Implementation of Non-Pipelined and Pipelined Data Encryption Standard Using Xilinx Virtex-6 FPGA Technology," IEEE International Conference on Computer and Information Technology 2010.

[10] Hamdan. O. Alanazi et.al, "New Comparative study between DES, 3DES and AES within Nine Factors" , Journal of Computing, vol. 2, Issue 3, ISSN 2151-9617, March 2010.

[11] Diaa Salama Abd Elminaam et.al, "Evaluating the Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.216–222, May 2010.

[12] Aamer Nadeem et.al,"A Performance Comparison of Data Encryption Algorithms," IEEE Department of computer Engineering, College of Electrical and Mechanical Engineering, 2005.

[13] Nazar A.Saqib et.al,"A Compact and Efficient FPGA Implementation of DES Algorithm", September 21, 2004.

[14] Arnaud Lagger et.al,"Implementation of DES Algorithm Using FPGA Technology", School of Computer and Communication Sciences Communication systems section, 2002.

[15] V. Pasham et.al,"High - Speed DES and Triple DES Encryption/ Decryption", XAPP270 (v1.0) August 03, 2001.

[16] Amit Dhir, "Data Encryption using DES/Triple-DES Functionality in Sparatan-2 FPGAs", WP115 (v1.0), 9 March, 2000.

[17] National Institute of Standards and Technology – Data Encryption Standard, FIPS PUB 46-3, October 1999.

[18] Wong, K et.al, " A Single-Chip FPGA Implementation of the Data Encryption Standard (des) Algorithm" IEEE Globecom Communication Conf., Sydney, Australia (827-832), 1998.

[19] Kaps et.al,"Fast DES implementations for FPGAs and its application to a Universal key-search machine" 5th Annual Workshop on selected areas in cryptography-Sac' 98, Ontario, Canada, Springer-Verlag, 234–247, 1998.

[20] Core (2000), F.D: URL: http://www.free-ip.com/DES/, 2000.