International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Synthesis of 64-Bit Triple Data Encryption Standard Algorithm using VHDL

Simran[1], Parminder Singh Jassal[2]

[1]M.Tech Student, Department of Electronics, Yadavindra College of Engineering, Talwandi Sabo, Punjab
[2]Assistant Professor, Department of Electronics, Yadavindra College of Engineering, Talwandi Sabo, Punjab

ABSTRACT

Data security is the most important requirement of today's world, to transmit digital data from one place to another. We need to secure the transmitted data at the transmitting end so that no unauthorized user can access it. To encrypt the data at the transmitting point and decrypt the data at the receiving point we need the communication security[8] . Only the authorized user can get back the original text, provided they have the secret key. Cryptography is a technique to transmit protected data between two points. The word 'Cryptography' was invented by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing. Cryptography is the study of mathematical techniques related to aspects of various information data security. It deals with protection of data on unsecured channel by altering the data in encrypt (coded)form. Basically, we have two cryptography techniques for digital data transfer, depending on how the encryption-decryption is carried out in the system, Symmetric Cryptography and Asymmetric Cryptography. DES, TRIPLE-DES, IDEA, AND BLOWFISH algorithms use symmetric cryptography technique. 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 synthesize TDES, which give higher operating frequency. In this paper we present, TDES synthesis in VHDL, in Electronic Code Block(ECB) mode, of this commonly used cryptography scheme with aim to improve performance. The design is simulated and synthesized in Xilinx ISE 14.7 with family Virtex-7 (XC7VX330t– 3ffg1157). Our design achieves a operating frequency of 114.33 MHZ.

Keywords: *Cryptography, DES, TDES, Encryption, Decryption, Implementation Results*

I. INTRODUCTION

In this modern era as the demand and the importance of exchanging valuable data over the internet is booming over electronics communication. The main need 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 concern is to get a higher operating frequency.

In [10], efficient and compact reconfigurable synthesis of the Data Encryption Standard (DES) algorithm [10] and synthesis using device VirtexEXCV400e.

In [11], a pipelined implementation in VHDL, in ECB mode, of this commonly used Cryptography scheme

with aim to improve performance, is given. using Altera Cyclone II FPGA as platform, design, verification and synthesis with a EDA tools provided by ALTERA. This design achieves a throughput of 3.2 Gbps with a 50MHz clock, is given.

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 performs an initial permutation (IP) on the entire 64 bit block of data. It is then split into Two, 32 bit sub-blocks,(Li and Ri) which are then passed into what is known as a Round which has 16 (the subscript i in Li and Ri indicates the current round)iterations[7]. There are 16 iterations of identical operations, called Function f, in which the input data are combined with the key. The basic operation of DES can be understood with the help of fig 1[2]. 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].

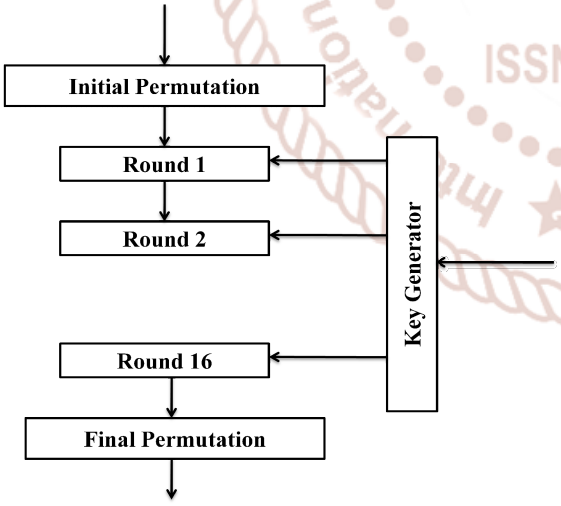

Fig.1- General structure of DES[2]

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 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

Algorithm Decryption Steps

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

B. TDES (Triple Data Encryption Standard)-

Triple Data Encryption Standard (Triple DES) uses a Symmetric key block cipher algorithm to convert original text into cipher text[3]. DES algorithm is used three times in Triple DES. Hence, there are 3 different keys(e.g. K1,K2,K3) to perform each application of DES. Therefore, it raises the key length to 168 bits(56 bit key each)/(excluding 24 parity bits, 8 from each key) and the keys are collectively known as the 'key bundle'. Triple DES uses DES three times that's why it have 48 rounds in it for more security and less prone to attacks. Triple DES uses a key length of 168 bits whereas a key length of 112 bits is preferred in TDES. 3 DES uses 64 bits of data block for encrypting the plaintext.

The main function of Triple DES is, to encrypt the plaintext with the first key(K1), decrypt the result of step 1 with second key(K2) and finally, encrypting the obtained result from step 2,with the third key(K3). Triple DES is defined by the function in figure (2) [14].

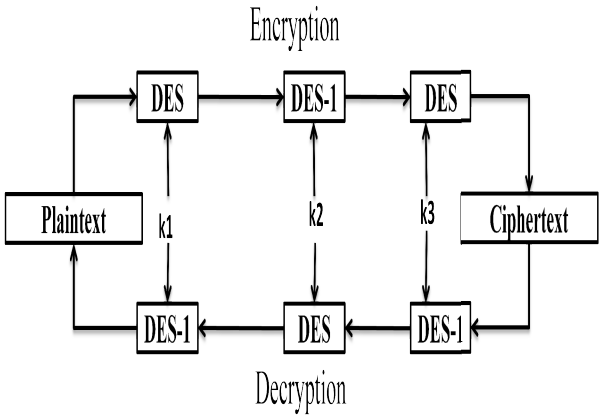

Fig 2:- TDES Algorithm working [14]

If we assume that **k1**, **k2** and **k3** are the 3 different keys and **C** to be the ciphertext and **P** to be the plaintext and **F** to denote encryption and **f** to denote decryption, then the encryption process of the Triple DES can be represented as

C = Fk3 [fk2 {Fk1 (P)}]……..equation. 1

In the same way, the decryption process of Triple DES can be represented as

P = fk1 [Fk2 {fk3 (C)}]…….equation. 2

III. SIMULATION RESULT

Encryption Simulation Waveform verifies TDES Encryption for following Key and Plain text values: The input key ,data input & decrypted output are as given. This Encryption Simulation Waveform verifies TDES Encryption for following Key and Plain text values:

TDES ENCRYPTION

- data in : FF00FF00FF00FF00
- data_out : 328DBFFA68CF0D06
- Key_1: 0000FFFF0000FFFF
- Key_2 : 00000000FFFFFFFF
- Key_3 : FFFF0000FFFF0000

TDES DECRYPTION

- data_in : 328DBFFA68CF0D06
- data_out : FF00FF00FF00FF00
- Key_1: 0000FFFF0000FFFF
- Key_2 : 00000000FFFFFFFF
- Key_3 : FFFF0000FFFF0000

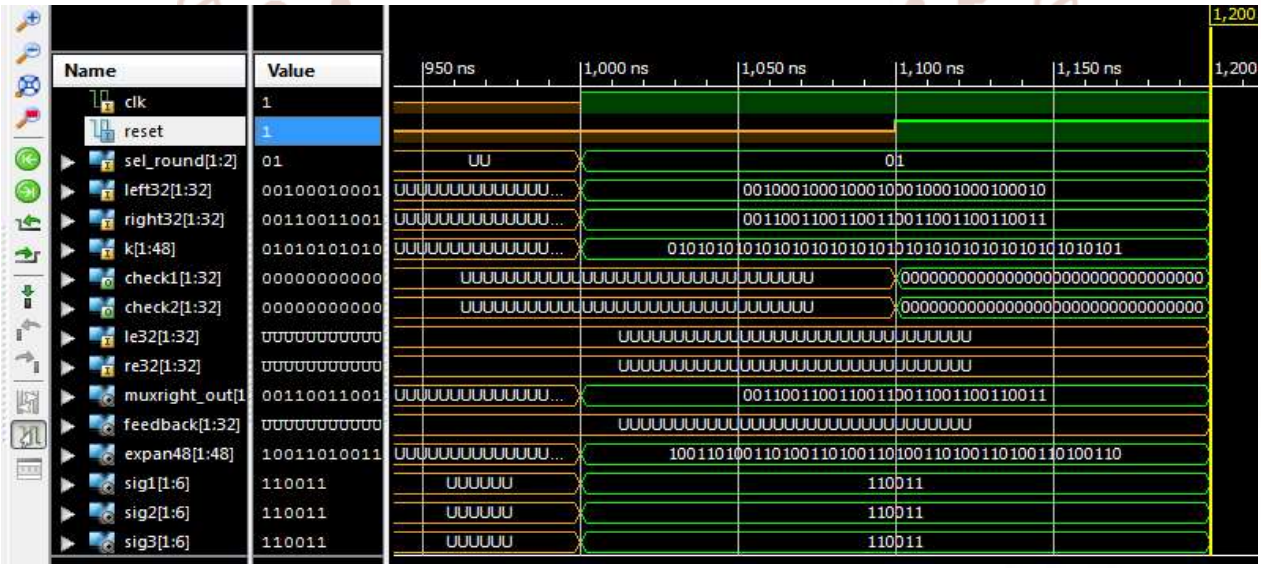

Fig 3 : TDES Encryption Simulation Waveform

IV. EXPERIMENTAL RESULTS

The design is simulated and synthesize in Xilinx ISE 14.7. The verified model is synthesized to get an high operating frequency. TDES implementation results are as given in table 1 :
As shown our work provides high operating frequency:

Table 1. TDES implementation Results

Author	Device	Frequency (MHZ)
[10]	XCV 400	47.7
Our work	XC6VLX75T	114.33

In this work, TDES is analyzed on XC6VLX75T device. The table depicts that the our work results in higher operating frequency.

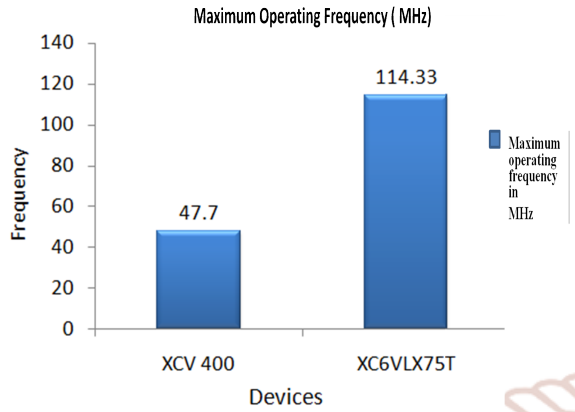

Fig 4. Comparision graph of TDES (Max. Operating Frequency)

V. CONCLUSION

This research presents the implementation of Triple Data Encryption Standards (TDES) algorithm using VHDL. The implemented design consumes fewer devices available on board which results better performance of algorithm.
As shown in Table 1, the frequency of TDES is higher than previous work, as compared to previous work.

VI. FUTURE SCOPE

For the future work, it is recommended that the input and plaintext can be taken using image or audio/video data. It is also recommended that the use of better FPGA board, which has better specification than Virtex-4 XC4VSX25-FF668 and has more number of input/output pins. The modification of Triple Data Encryption Standards(TDES) algorithm can also be done to get better security and reduction in total Encryption time, area and frequency etc.

REFERENCES

1. M. Breezely George and S. Igni Sabasti Prabu," Secured Key Sharing in Cloud Storage Using Elliptic Curve Cryptography", Springer India 2016.
2. Anilekha Thampi V V, Raju K Gopal," A Review on Different Encryption Algorithms for a Wellness Tracking System", Proceedings of 2015 Global Conference on Communication Technologies (GCCT 2015), IEEE 2015.
3. Parminder Singh Jassal et al., International Journal of engineering and technical Research ISSN: 2321-0869,volume-3,Issue-5,May2015
4. Mandeep et al., International Journal of advanced research in computer science and software engineering 4(1),january-2014,pp.667-672.
5. P. Kitsos, S. Goudevenos and 0. Koufopavlou," VLSI IMPLEMEN-TATIONS OF THE TRIPLE-DES BLOCK CIPHER",IEEE2003.
6. Herbert Leitold, Wolfgang Mayerwieser, Udo Payer, Karl Christian Posch, Reinhard Posch, and Johannes Wolkerstorfer,"A 155 Mbps Triple-DES Network Encryptor", Springer-Verlag Berlin Heidelberg 2000.
7. "Data Encryption Standard," Federal Infonnation Processing Standards Publication No. 46, National Bureau of Standards ,January15,1977 .
8. V. Pasham et. al, "High - Speed DES and Triple DES Encryption/ Decryption", XAPP270 (v1.0) August 03, 2001.
9. D.Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks", IBM J.RES.DEVELOP. VOL.38 NO.3MAY,1994.
10. Shivangi Vajpayee et al, Int.J. Computer Technology & Applications, Vol3(3),1015-1022.
11. Rosal, E.D. and Kumar, S. (2017) A Fast FPGA Implementation for Triple DES Encryption Scheme. Circuits and Systems, 8, 237-246.
12. Venigalla et.al.," implementation of triple des block cipher using VHDL", International Journal of Advances in Engineering & Technology, March 2012.
13. Akash Kumar Mandal et.al, "Performance Evaluation of Cryptographic Algorithms DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012.
14. O P Verma et.al, "Performance Analysis of Data Encryption Algorithms", IEEE International Journal of Computer Applications, Vo1.42, No.16, March 2011.
15. Miles E. Smid and Dennis K. Branstad, "The Data Encryption Standard: Past and Future," in Gustavus.