Hardware Implementation of more Efficiant TDES on FPGA by Pipelining using VHDL Language

Rohit Neelam[1], Deepika Soni[2]

[2]*Ass Prof. Deptt. of Electronics and Communications*

Gyan Ganga Institute of Science and Technology, Jabalpur, India

Abstract - We live in the world of Technology in which digitization is everywhere. In this modern era security is most important criteria in our daily life. No one wants to share their personal documents/messages with others. Instead of security, speed is also an important criteria. Everyone wants to complete/finish their work efficiently & in less duration of time. By taking all these parameters our research is based on TDES technology which is used for encryption & decryption of the message/data. TDES is the advance encryption-decryption methods which is using nowdays in most of the applications. This research is based on speed of the system. If the speed is good then all the work would be done efficiently & in a fast manner. In this research work, we implemented TDES on cyclone II & result is compared with the previous work. Here speed is most important criteria. Our work showed the better result than before.

Index Terms: Cryptography, DES, TDES, Cyclone II, FPGA.

I. INTRODUCTION

We all know that this is world of science & Technology. A world where digitization is everywhere. If we walk a single step a new technology is standing ahead of us. Each & every minute of day, the technology is increasing & the speed of the processing is also increasing. Day by day we all face a new challenge & get aware of new things. There are also most of the things by which we all are not aware with. So, Just read & learn more & more. The more we see, more we grasp & if more we work with than more we learn.

In our modern society, we all are using new technology like mobile phone, Laptops, Digital Watches etc & in office purpose most essential thing we should learn is E-mail writing & more messaging share apps. It is so because most of the conversion is done by E-Mail & messaging only. If we require sharing some document then mailing is important factor. If we require to share piece of message then nowadays whatsapp is using with very high demand. But why we all are discussing this? What are main criteria behind this thing? If we wish to piece of message then most essential thing a person can think is my message is visible to 3rd party or not? Is my message is secure or not? Do anyone would able to decrypt my message?

A. CRYPTOGRAPHY

Cryptography is a procedure to convert plain message to cipher-message to make the message more secure. It is based on different protocols so that the third party would not capable to fetch our data & our data is more secure. In simple means, technique to convert readable message to apparent nonsense at transmitter side & then again the secured message is transformed in readable message at receiver side is cryptography. Due to this if a person is trying to extract the message then that person would able to see only the encrypted message which is not readable to any person. And that non-readable message is just a waste for him.

B. TDES

TDES[1] is most leading encryption standard using nowadays. It uses DES three times. This algorithm is far better than the DES algorithm. It is so because the Key length used in DES is 56 bit. But the TDES uses DES 3 time's means the key length is increased by

56 X 3 = 168-bits

The Key length of TDES is 168 bits. Due to key length the TDES is more defended then the DES algorithm & also used in many applications. The block diagram of TDES is shown below.

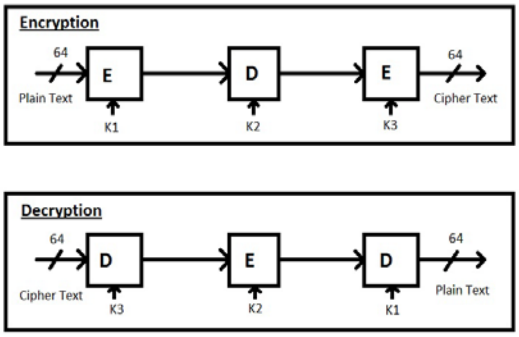


Fig 1: Triple DES-Block Diagram

TDES uses DES[5] three times for encryption likewise for decryption. We are using 3 block of DES to perform operation of TDES. In above figure, we can evaluate that there are two blocks 1st block for encryption & 2nd one for decryption, one is cipher & other block is deciphered. Lets first looks at the cipher block. In cipher block first plain-text is enforced to DES encryption block. Where Encryption of plain message is done with key K1. When plain-text transformed into cipher-text then result of 1st block conveyed to 2nd DES block which is doing the decryption operation. Here is key point if we do the decryption with like's key then here we get plain-text & TDES transformed into DES. But here we decrypt data with different key K2. Due to this the readability of the plain-text is more difficult. After the 2nd block, its result conveyed to block 3 in which DES is again performing Encryption operation. Here encryption operation is done by different key K3. After this we get our final output Cipher text which is of 64 bit.

This is all about encryption of TDES. In the second block TDES decryption is shown. Here cipher text of 64-bit which we get in encryption side conveyed to the first block of DES which is performing Decryption operation with K3 key. Then output of 1st block in decryption block conveyed to 2nd block which is doing encryption now but with different key K2. Then output of 2nd block conveyed to 3rd block which again performing decryption with key K1. After this we get our plain message.

Here we can see that decryption is just reverse of encryption method & here keys are also get reversed.

II. TDES ALGORITHM

A. ENCRYPTION

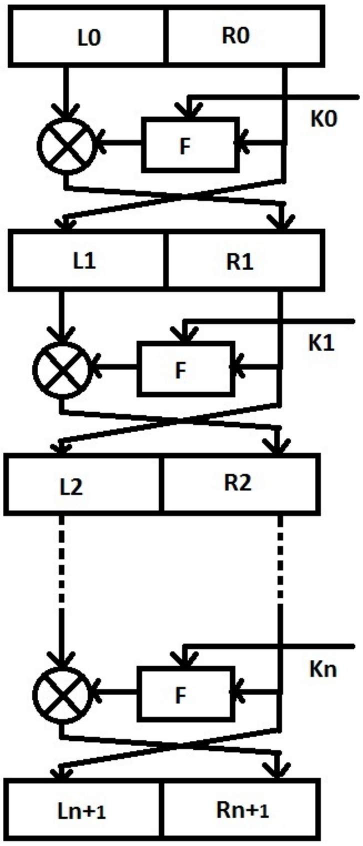


Fig 2: Encryption in rounds

The above diagram is the encryption of rounds. Here the value of n varies from 0 to 15. So the values of keys are K0, K1….to K15. Total 16 keys used for 16 rounds & all the keys are distinct from one another. Here Ln+1 & Rn+1 are the registers which are used to stores o/p bit of the pervious processing. There are total 3 DES Block used in TDES[3]. This is diagram of one block of DES.

B. DECRYPTION

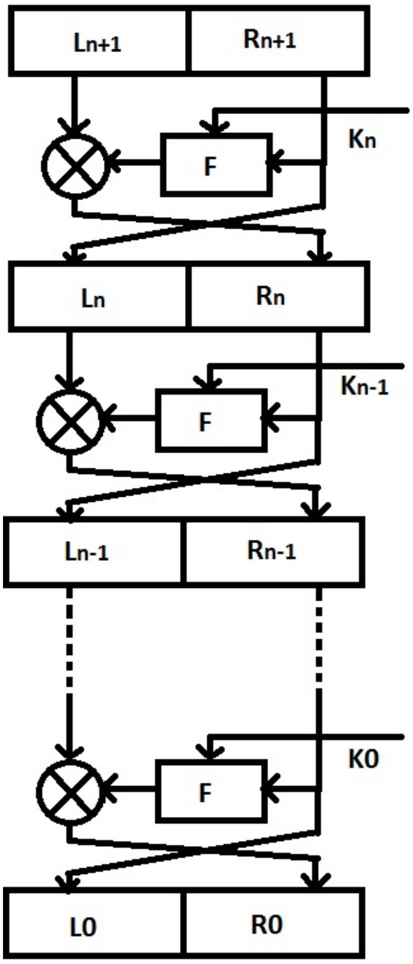
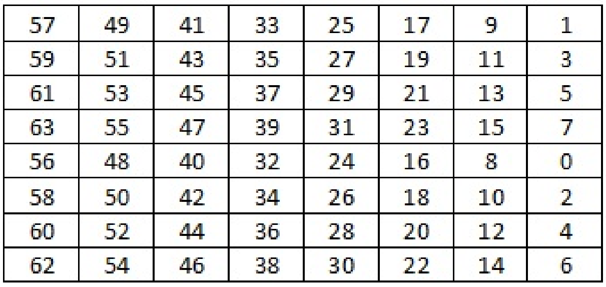


Fig 3: Decryption in rounds

Decryption is converse technique of encryption technique. This is why we are using Feistel-structure in TDES[4]. As this is reverse process, the keys & rounds get reversed. Here first we decrypt cipher-text by key 16 (Kn) after this in 2nd round we decrtpt with key 15 (Kn-1) & so on. & finally we get the plain message at the end after final permutation is done.

C. INITIAL-PERMUTATION (IP) BLOCK

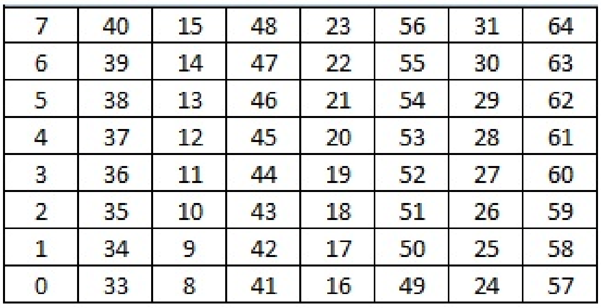
Table 1 shows initial-permutation block which would perform before the 16 rounds in feistel structure. It is initial block of feistel structure. The above table specifies that the 2nd bit (1) is copied to the 8st bit of o/p, 60th bit (59) is copied to the 9th position of the output & similarly 15th bit is copied to the 63 position of the output. This shifting of bits are fully depend upon programmer. How the programmer wants to shuffle the bits. If the programmer wants to copy the 58th bit at another position then he/she can do so. More the shuffling more the data would be secure.



57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7
56	48	40	32	24	16	8	0
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6

Table 1: Initial permutation

B. FINAL PERMUTATION (IP-1)



7	40	15	48	23	56	31	64
6	39	14	47	22	55	30	63
5	38	13	46	21	54	29	62
4	37	12	45	20	53	28	61
3	36	11	44	19	52	27	60
2	35	10	43	18	51	26	59
1	34	9	42	17	50	25	58
0	33	8	41	16	49	24	57

Table 2: Final Permutation

Final permutation is inverse of initial-permutation block. This is shown in Table-2. This block execute after the 16 rounds in feistel-structure for more shuffling. This block is fully depend on initial permutation. How the bits get shuffled in the initial permutation.

C. PERMUTATION (P)

PERMUTATION – BOX				
1ST bit	15	6	19	20
5th bit	28	11	27	16
9th bit	0	14	22	25
13th bit	4	17	30	9
17th bit	1	7	23	13
21st bit	31	26	2	8
25th bit	18	12	29	5
29th bit	21	10	3	24

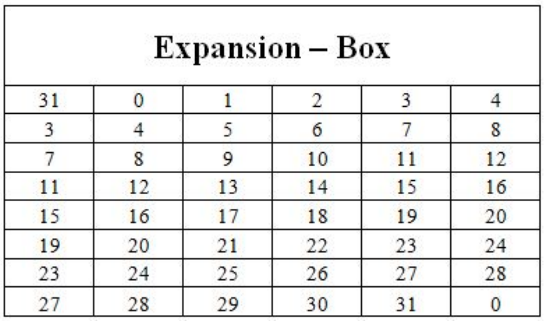
Table 3: Permutation Block

The 32 – bit output of the S –box substitution is permuted according to a P –box. In this block bit by bit mapping is done between input bits & output bits; no bits are used 2 times & no bits get ignored. This is termed as straight permutation or just a permutation. This is shown in table 3.

D. EXPANSION PERMUTATION (E)

This box comes in the F-Block of Feistel-structure. In this box 32 bits of Ri-1 is applied & the output we get is 48-bit which is get XOR'ed with the 48-bit key. Here 32 bits are expanded to 48-bits. In this 16 bits are copied ones to the output & 16 bits are copied 2 times at the output. In above table, we can convey that 11th bit is duplicated at the 17th & 19th position & 13th bit is copied at one place only that is 21st position. It is also called expansion permutation because this block also change the location of bits. The two main purpose of this block is

1) It give 48-bit output for XOR-operation with key.
2) It provide 48-bit output which is used to get compressed by the S-Boxes.



Expansion – Box					
31	0	1	2	3	4
3	4	5	6	7	8
7	8	9	10	11	12
11	12	13	14	15	16
15	16	17	18	19	20
19	20	21	22	23	24
23	24	25	26	27	28
27	28	29	30	31	0

Table 4: Expansion Box

Dependency of output bit over input bit is spread faster. This is defined as Avalanche effect.

III. TDES PIPELINING

A. LOOP UNROLLING & PIPELINING

Sixteen copies of the rounds were made to unroll the loop. This is done for increase the speed. The data is pipelined through sixteen stages due to this speed of system is increased by the factor of 16. Figure 20 is showing critical path in rounds. A multiplexer is using in the circuit to select whether the encryption is done or decryption of data is done. If the select line bit is 0 the decryption process would take place & if the select line bit is 1 the encryption would carried out. Then selected bits are Exclusive OR'ed by the RHS bits (Ri) & six bits range used to start the working in S-Boxes. One bit of S-Box is shown by the 4 LUT's & F5 MUx is used for the selection of bits. Then the output bits from S-Box are permutated Exclusive OR'ed by the Li bit & get stored in the pipelined registered.

B. LUTS MAPPED TO S-BOXES

Cyclone II LUTs can be composed as 16X1 ROM. As we know that our design contain many number of constant S-Boxes. Each & Every bit in the S-Box consists of 64-bit word look up table. The 4 i/p lookup table/ 4 LUTs composed as ROM by the use of Case statement in the VHDL programming language. The Constant terms of S-Boxes are composed as 4 LUTs & directly connected to F5 MUX to fetch the output directly with the help of select lines. The F6 MUX is not directly connected to the 4 LUTs because it's used for XORing selected bits with the Left hand side (Li) Block.

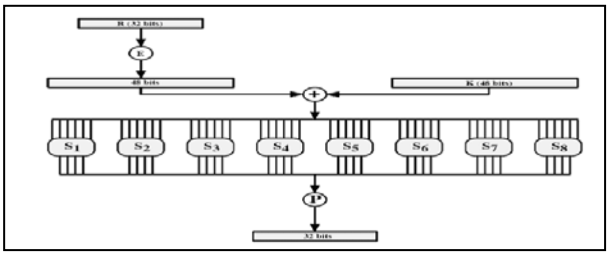


Fig 4: Calculation of f(R, k)

This is all about the LUTs mapping with S-Boxes. After performing exclusive-OR operation with 48-bit key then the output of S-Box is send over 8 S-boxes. Each S-Box input defined by 6-bits, output defined by 4-bits & there is total number of 8 S-boxes. Therefore, total memory used for eight S-Boxes are 256 bytes. These 48-bits are divides into 8 blocks of 6 bit each. Each different block is operated by the different S-Box. The first block of bits are operated by the 1st S-Box, the second block of bits are operated by the 2nd S-Box & so on upto eight S-Box.

C. PIPELINING

Each round of DES is pipelined in three phases to upgrade execution. This builds the inactivity to 48 cycles. The information way is isolated from key generation due to this the logic levels reduces between resulting pipeline stages. The schematic for one round of DES is appeared in above figure.

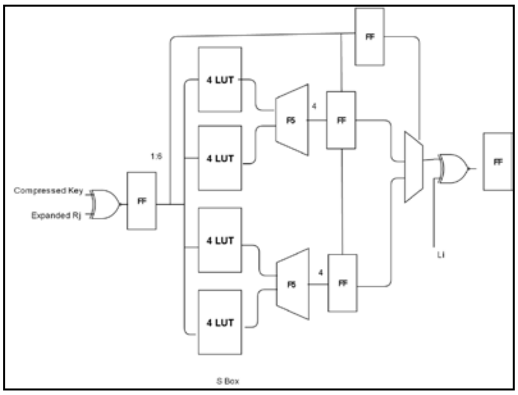


Fig 5: Single-Round Data Path

D. GENERATION OF KEY

The 64 bit of initial key is get permuted & get several number of shift operation. After the shifting operation 2nd permutation is done for each & every round. This key generation[12] process is independent of rounds in the DES blocks. It is done with 3-stage pipelining to satisfied the pipelining in rounds in DES Algo. The 3-stage pipelining is accomplished by designing LUTs as Shift Registers (SRL16) followed by one flip-flop. Shift register is configured by the Cyclone LUTs & the one to 16 shift register for each & every LUTs defined by user. Cyclone-II devices should allow cascading of 8 SRL16s in the single CLB (4 slices, 8 LUTs) to create 128-bit shift register. The SRL-16, required to create 2-stage pipelining & 3rd stage pipelining is created by the flip-flop which is followed by the SRL16. This presents Place & Route tools with great adaptability in setting these SRL-16s & flip-flops to accomplish better speed for system. Key-generation for a round is appeared in Figure 6

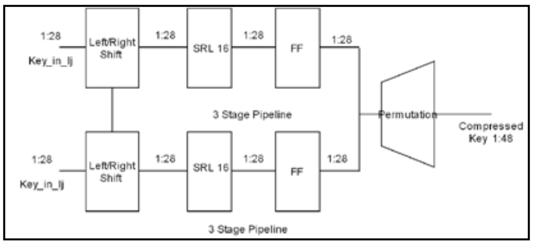


Fig 6 : Single Round Key Generation

Three copies of DES are instantiated to realize Triple DES implementation. The latency of Triple DES is 144 cycles, i.e., 48 cycles for each copy of DES.

IV RESULT

	Qian Wang et all[2]	**our work**
SPEED (frequency)	6.25 MHZ	11.25 MHZ

Table 5: Comparison 1

Above table is comparison table of reference paper 1 which was published in IEEE in 2013. In this paper, speed/frequency is calculated at the 50 MHz internal clock. The result of the Ref[1] is 6.25 MHz. our implementation is on the 500 MHz internal Clock. The result comes is 119.5 MHz frequency but when we implemented on the 50MHz clock the result we get is 11.25MHz which is just double of the previous work.

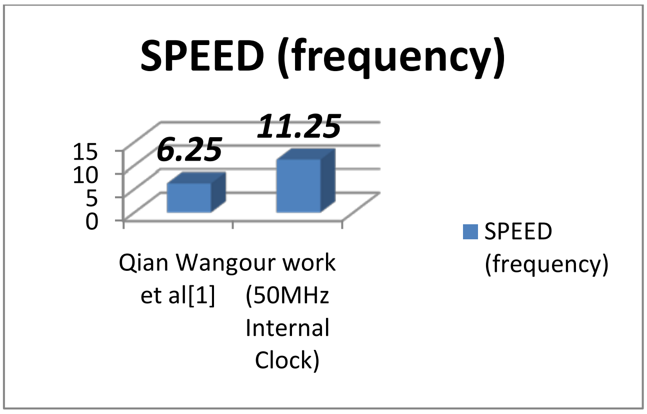
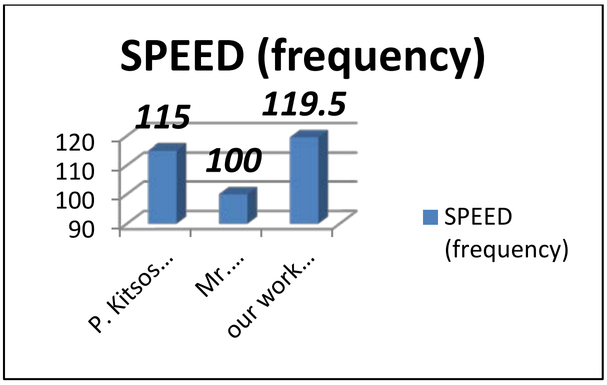


Fig 6: Graph of Comparision-1

	P. Kitsos et all[3]	**Mr. A.Kaleel Rahuman et all[4]**	**our work (500MHz Internal Clock)**
SPEED (frequency)	115	100	119.5

Table 6: Comparison 2

Above table is comparison table of reference paper 2 & reference paper 3 which was published in IEEE in 2003 & IJCSMC in 2014 respectivly. The speed calculated for TDES in this paper was 115 MHz &100 MHz respectively. our speed calculated is 119.5 MHz which is much better that the previous work.



.

Fig 7: Graph of Comparision-2

V CONCLUSION

The proposed implementation of TDES provide high-speed performance with very compact hardware implementation. It is a flexible solution for any cryptographic system and security layers of wireless protocol. Measurement results and comparisons between the proposed and previous hardware implementations are presented that shows quite encouraging results.

In this work a compact hardware implementation of Triple DES was presented. The design was implemented in real hardware with Cyclone II FPGA.

TDES is used in Electronic Payment industry, Microsoft OneNote, Microsoft Outlook 2007 and Microsoft System Center Configuration Manager 2012 used TDES technology to make the data password protected.

The speed of the system is comes as119.5 MHz at 500 MHz internal clock and 11.95 MHz at the 50MHz internal clock which is just double compared to the previous work.

REFERENCES

[1] Luminita Scripcariu “A Study Of Method Used To Improve Encryption Algorithms Robustness” Published On IEEE in July 2015.

[2] Qian Wang, Xiangmin Zhang, Xiangyu Li,Jun Guo, Liji Wu “Efficient Countermeasures against Fault-Attacks for 3-DES Crypto-Engine in Bank IC-Card”,IEEE,2013.

[3] S. Goudevenos, P. Kitsos & 0. Koufopavlou has proposed “VLSI Implementation of Triple DES Block Cipher”, IEEE 2003.

[4] Dr. G.Athisha, Mr. A.Kaleel Rahuman “Performance Analysis Of Reconfigurable Crypto-Processor For Security & Privacy In Communication-Networks”,IJCSMC,2014.

[5] Mohammed M. Alani “DES96 – improved DES Security” Published On IEEE in June 2010.

[6] Jose A “TDES Implimentation In A Reconfigure Computing Environment” Published On IEEE in March 2008.

[7] E. Biham and A. Shamir, "Differential Cryptanalysis of the full 16-round DES", in Proc. OjCRYPTO'92, page 487.

[8] J. Katz, Y.Lindell, “Introduction to Modern Cryptography”, second edition, CRC Press, 2015.

[9] J. Kelsey, B. Schneier and D. Wagner, "Key-schedule cryptanalysis of IDEA, GDES, GOST, SAFER, and Triple-DES," in Advances in Cryptology, Proceedings Crypto '96, LNCS 1109, N. Koblitz, Ed., Springer-Verlag, pp. 237-252, 1996.

[10] E. Biham, A. Shamir, “Differential Cryptanalysis of the Data Encryption Standard”, Springer Verlag, 1993.

[11] William M. Daley, "Data Encryption Standard (DES)", U.S. DEPARTMENT OF COMMERCE/National Institute ofStandards and Technology, October 1999.

[12] W. Stallings, Cryptography and Network Security: Principles and Practice, 4th ed , Prentice-Hall, 2006.