An Efficient Implementation of Enhanced Key Generation Technique in Data Encryption Standard (DES)Algorithm using VHDL

Ms. Punam Milind Chabukswar, Mr. Manoj Kumar, Mr. P. Balaramudu

***Abstract*—Cryptography is the way toward securing message to maintain a strategic distance from an unapproved hacking of information. Secured Key assumes vital part in cryptography. For expanding the level of security in any correspondence framework this venture proposed an Enhanced key generation unit. The framework proposed here three other that direct keys era approaches to make key generation more grounded are client produced key, second one by utilizing LFSR which is great key stream generator, third is by utilizing chaotic encryption and fourth is 2's supplement. Another part is DES calculation and control unit is likewise intended for controlling the 16 round of DES of encryption and decoding process. In the usage of DES encryption and decoding calculation, a multiplexer-based engineering is utilized to execute the substitution operations (S-Boxes). These proposed engineering is displayed in the VHDL outline dialect and combined in the Xilinx Virtex-xc6vlx75t-3ff484 field-programmable gate array (FPGA) device.**

***Index Terms*—Cryptography, DataEncryption, Decryption, Direct key, Chaotic Encryption technique, LFSR, 2's comlement**

I. INTRODUCTION

Cryptography is the procedure of furtively composing implies scrambling the information which is not in intelligible arrangement. The need of cryptography is emerges to keep the private data from unapproved individual. Security of the information or framework is relies on upon both cryptographic calculation and key utilized for encryption/decryption. Cryptography is required in different areas like banks, military, railroads, media transmission and so forth. In electronic reserve exchange like ATM cards, PC passwords, electronic passwords likewise require the security. Cryptography has wide region of extension since this procedure has capacity to give security against different assaults. Cryptography principally incorporates two sections i.e. encryption and decoding, encryption is the way toward changing over of plain content to figure content and unscrambling is the other way around to encryption as appeared in figure 1

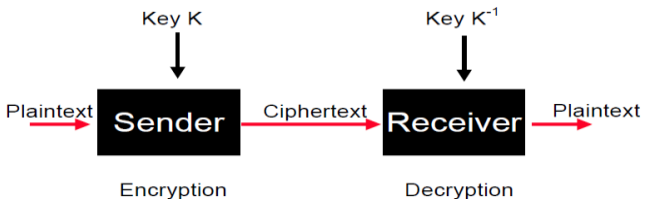

Figure 1: Block diagram of Cryptographic Model

II. LITERATURE SURVEY

J. G. Pandey, AanchalGurawa, Heena Nehra, A.Karmakar give the FPGA Implementation of an Efficient VLSI Architecture for Data Encryption Standard count based encryption/translating engine.[1]

Data Encryption Standard (DES) is a cryptographic standard that was proposed as the count for secure and riddle things in 1970 and was gotten as an American government standard by National Bureau of Standards (NBS) in 1973.

CRS Bhardwaj, Elaborate the Modification Of DES Algorithm analyzes the change of DES computation, which is the examination of data encryption, an advancement that obliges a protected, secure, and private information trade.

Ali Makhmali, Hajar Mat Jani illuminates the execution and respond in due order regarding handle these two issues. These issues at first drove us to play out a close audit on a couple of encryption computations, and in this way, to find the most fitting one; and second, to find the best organization structure of data to ensure a sensible level of security for the clients of the online application. [4]

Nimmi Gupta, Data Security is a basic parameter for the undertakings. It can be refined by Encryption estimations which are used to prevent unapproved access of information[5].

Karthik S. in addition, Muruganandam A., portrays a framework for riddle correspondence using cryptography.[6]

Sombir Singh, Sunil K. Maakar, Dr.Sudesh Kumar developed the DES count the transposition framework is added before the DES computation to play out its procedure.[7]

A. Present day cryptography

The route toward changing over plain substance to figure content is known as encryption and the count which encodes the data is known as encryption computation. In the present-day cryptography, a mix of both open key and regular symmetric cryptography is used. The reason behind this is open key encryption arranges are computationally genuine versus their symmetric key accomplices.

III. SYSTEM DEVELOPMENT

A.DES Algorithm Description

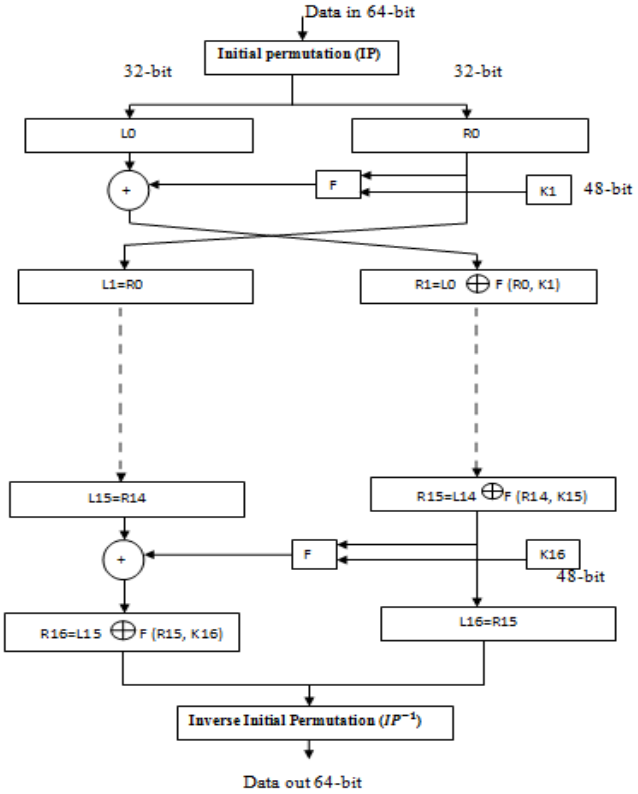

Figure 2: DES algorithm description.

DES (Data Encryption Standard) Cryptographic algorithm is a block cipher calculation which utilizes symmetric key cryptography. It utilizes 64-bit key for both scramble and unscramble 64-bit plain text and cipher text message individually. DES algorithm portrayal is as appeared in fig. 2. It chips away at 64-bit plain text to create 64-bit figure message in this way 64-bit plain text is given as information contribution to perform initialpermutation (IP) first at that point key ward stage and finally last stage which is opposite beginning changefinal permutation which is inverse initial permutation i.e.IP-1. DES calculation performs 16-rounds of operation to deliver 64-bit yield information. The execution of DES requires four essential operations mostly XOR, move, LUT (Look up table) and stage which are easy to actualize in equipment. As appeared in figure 3, 64-bit information input is at first get permuted by IP and after that get parts into two equivalent amounts of right half (R0) and left half (L0), each is 32-bit long. Right half in first round will be the left 50% of the following round and right 50% of next round is acquired by initially extending 32-bits to 48-bits by utilizing extension work in that we grow it by rehashing a few bits then this extended 48-bit are XORed with 48-bit key and after that outcomes sustained into eight 6-bit substitution boxes (S-boxes) which changes over 48-bit contribution to 32-bit yield i.e. 6-bit sbox gives 4-bit yield to frame 8 4-bit boxes lastly stage is done on these 32-bits. In next stage this 32-bit permuted yield is get XORed with first right half 32-bits to get next right half 32-bits. Function F in the key ward stage is the most essential Function of the DES algorithm and its operation is as appeared in figure3. Distinctive operations like expansion, substitution, permutation and also XOR operation with the 48-bit key are occurred.

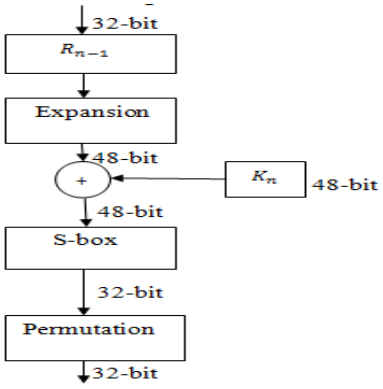

Figure. 3 DES function F details

B.Linear feedback shift register

LFSR is a decent stream generator. A LFSR comprise of shift register and a linear feedback function as appeared in figure. In that shift register is a succession of M flip failures BM to BM-1 and each flip slump holds single bit. Flip failures are instated to a M-bit word. BM is a direct capacity of B0,B1,B2,… ..,BM-1. LFSR is separated in light of the kind of sources of info and yields. Here LFSR is utilized to create arrangement of keys.

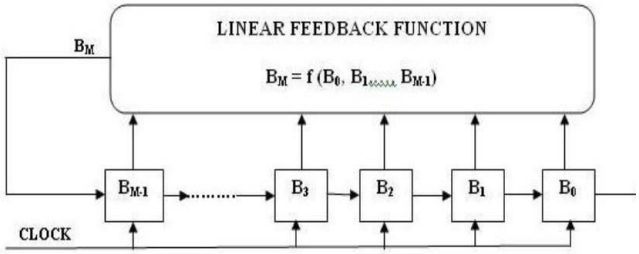

Figure 4: Block diagram of linear feddback shift register

C. Chaotic encryption

In chaotic encryption 'chaos' signifies 'a condition of confusion'. Here framework utilizes one dimensional chaotic signal which is utilized to cover helpful data and make it unrecognizable by aggressors. To get abnormal state of security confused encryption is utilized to scramble computerized information. Here particularly framework utilizes piecewise straight one dimensional disorganized guide. This framework has an ever-increasing number of complex progression subsequently it has wide applications in the field of correspondence. So, the piecewise straight one dimensional chaotic map is utilized for dynamic key era unit. Its condition is as per the following:

$$x_{n+1} = 1 + 2x_n, \text{ for } x_n < 0$$
$$= 1 + 2x_n, \text{ for } x_n \geq 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Sequence is produced by logistic map. It is non-occasional and joining under starting condition. Chaotic sequence is not pseudorandom, but rather really stochastic, so solid key is get created utilizing these qualities.

D. 2's complement

This can be likewise another alternative used to create more generations of keys.

Its condition is as per the following: It's equation is as follows:

2's complement=1's complement + 1..... (2)

1's complement =(2^n) – N

IV. PROPOSED DESIGN

A. Dynamic key generation block

As per this the examining the key ought to be difficult to the point that there is no compelling reason to shroud the encryption and decryption algorithm, however in DES algorithm, 56-bit key is the principle shortcoming in light of the fact that there are presently 256 conceivable keys are accessible which are effortlessly get split by ""“brute force attacks ". It includes attempting each of the 256 keys out of that 4 are powerless, 12 are semi frail and 48 are conceivable feeble keys. So, to enhance the execution of the DES calculation and upgrade security we need to build number of conceivable methods for key era. We proposed an improved key generation unit in DES to expand number of conceivable methods for key era. In this unique key generation unit, it incorporates two squares i.e. key produced by client and LFSR. By utilizing key created by client there are 256 conceivable keys are accessible yet subsequent to moving through LFSR there are more 256 keys are get produced implies at long last there are add up to 2112 ways are accessible. For making more disarray in key generation it can be created by any of the above strategy.

To expand number of methods for key generation more than 256, we proposed a dynamic key generation in DES. As appeared in figure dynamic key generation unit comprise of four squares named coordinate key, LFSR, chaotic encryption and 2's complement. Here we are not going to give the first key contribution to the disorganized encryption piece; disorderly encryption block creates the distinctive mixes of keys consequently at each clock cycle.

V. SIMULATION RESULT

DES algorithm is implemented with VHDL and simulated in RTL level with Xilinx ISE 12.3 simulator and simulation results are as shown in figure.

In simulation results both encryption and decryption results are shown when decipher is 0 then encryption takes place and when decipher signal is 1 decryption takes place. Encryption results are get after 16 clock cycles and this encryption result is decrypted using same key to get original plaintext data.

As we are using multiplexer, mode selection is based on the select input given when select input S is “00” then direct key is get selected, for S “01” LFSR is get selected, for S “10” chaotic encryption is selected and for S “11” 2’s complement is get selected and we get the different simulation results for different modes as shown in figures below.

For encryption we used input value of 64-bit input value indata 8000000000000000 and 64-bit key inkey 0000000000000000. For decryption we used input value as its encryption output value and same key. Simulation results for encryption and decryption are shown in figures below.

Figure 5.1 shows direct key generation unit result similarly Figure 5.2 LFSR technique for key shuffling, Figure 5.3 for Chaotic Algorithm and Figure 5.4 for 2’s Complement used for key generation. In each simulation result figure (a) indicates encryption and figure (b) indicates decryption.

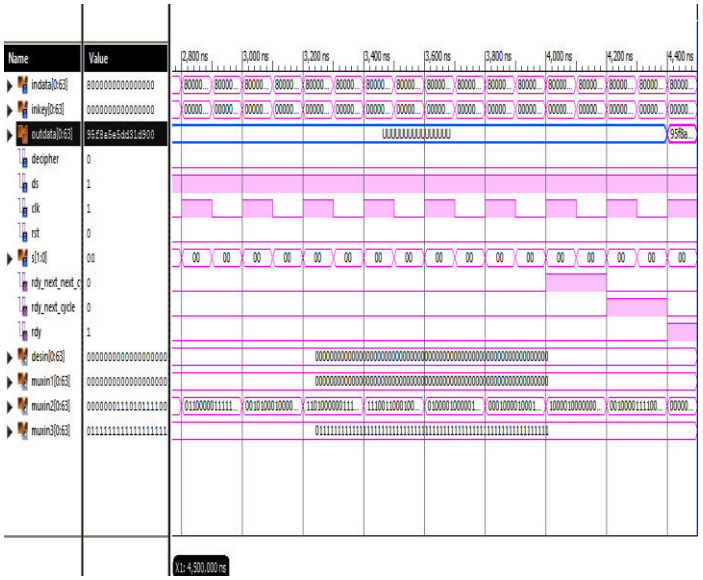

Figure. 5.1(a) Simulation results for direct key

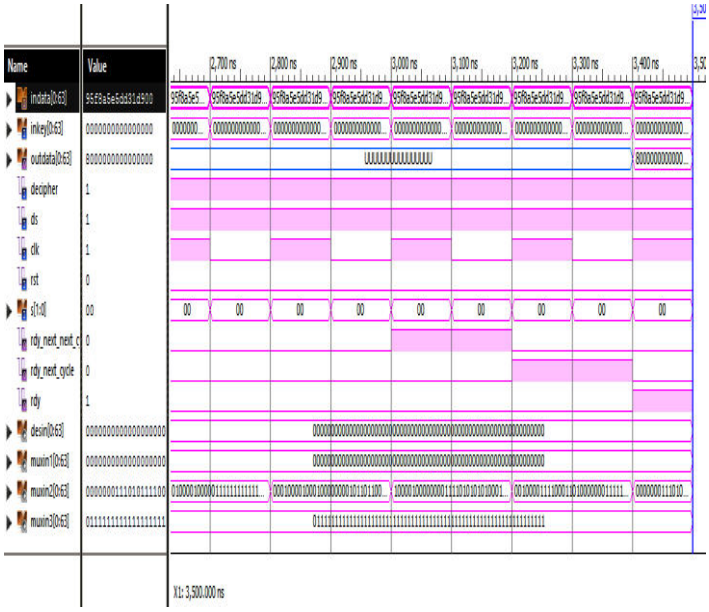

Figure. 5.1(b) Simulation results for direct key

Figure. 5.2 (a)Simulation results for key generated by LFSR

Figure. 5.2 (b)Simulation results for key generated by LFSR

Figure. 5.3(a) Simulation results for key generated by chaotic encryption

Figure. 5.3(b) Simulation results for key generated by chaotic encryption

Fig. 5.4(a) Simulation results for key generated by 2's complement.

Fig. 5.4(b) Simulation results for key generated by 2's complement.

FPGA Resource Utilization: -

Sr. no.	Resource Name	Resource Utilization	Utilization(%)
1	Software Tool-Xilinx ISE design Suite	12.3 Build –Logic Edition	-
2	Top level entity name	Topdes112	-
3	Processor Family	Virtex6	-
4	Device	xc6vlx75t-3ff484	-
5	Slice Registers	448/93120	1%
6	Slice LUTs	544/46560	1%
7	Bonded IOBs	201/240	83%
8	BUFG	1/32	3%

VI. CONCLUSIONS

The security of any type of algorithm is dependent on the secrecy of the key. Due to the dynamic key generation unit secrecy of the key get increased. Simulation results are shown for both encryption and decryption. Using proposed design, we can achieve high speed and reduced logic complexity which gives enhanced DES algorithm. According to this enhanced DES algorithm has broad application area in secure data communication and transmission.In future, we can execute this framework for greater security in various applications, for example, Smart card security Database administration framework, Set top box, Wireless correspondence security, Content insurance.

ACKNOWLEDGMENT

I thank our colleagues from SVCET Rajuri who provided insight and expertise that greatly assisted the dissertation.
I would like to show our gratitude to the prof. P. Balaramudu (Vice Principal) for sharing their pearls of wisdom with us during the course of this dissertation. We are also immensely grateful to Prof. Manoj Kumar (PG Coordinator and HOD of E&TC Department) for their comments on an earlier version of the manuscript.

REFERENCES

[1] J. G. Pandey, Aanchal Gurawa, Heena Nehra, A. Karmakar, An Efficient VLSI Architecture for Data Encryption Standard and its FPGA Implementation, International Conference on VLSI Systems, Architectures, Technology and Applications (VLSI-SATA),2016 .

[2] William Stallings, Cryptography and Network Security Principles And Practice, Prentice Hall publication, page no.51-56, 2011.

[3] CRS BHARDWAJ, Modification Of Des Algorithm, International Journal Of Innovative Research & Development, Nov 2012, Vol 1,Issue 9,Page 495

[4] Ali Makhmali, Hajar Mat Jani, Comparative Study On Encryption Algorithms And Proposing A Data Management Structure, International Journal Of Scientific & Technology Research, Volume 2, Issue 6, June 2013.

[5] Nimmi Gupta, Implementation of Optimized DES Encryption Algorithm upto 4 Round on Spartan 3, International Journal of Computer Technology and Electronics Engineering Vol 2 , Issue 1, Jan2012.

[6] Karthik .S1, Muruganandam .A Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System, International Journal of Scientific Engineering and Research, Volume 2 Issue 11, November 2014

[7] Sombir Singh, Sunil K. Maakar, Dr.Sudesh, Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques, International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, Volume 3, Issue 6, June 2013.

[8] W. Stallings, Cryptography and Network Security Principles and Practice, 5th ed. Prentice Hall, 2011.

[9] S. Vaudenay, A Classical Introduction to Cryptography: Applications for CommunicationsSecurity,Springer Science & Business Media, 2006.

[10] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," IEEE Design & Test of Computers, vol. 24, no. 6, Test of Computers, vol. 24, no. 6.

[11] M. E. Smid and D. K. Branstad, "Data encryption standard: past and future," Proc. of the IEEE, vol. 76, no. 5, pp. 550-559, 1988.

[12] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard. Springer Science & Business Media, 2012.

[13] S. Kelly. (2006, Dec.) Security implications of using the data encryption standard (DES). [Online].
https://tools.ietf.org/html/rfc4772

[14] O. P. Verma, R. Agarwal, D. Dafouti, and S. Tyagi, "Peformance analysis of data encryption algorithms," in 3rd Int'l Conf. on Electronics Computer Technology (ICECT), vol. 5, Kanyakumari, 8-10 Apr. 2011, pp. 399-403

[15] C. Patterson, "High performance DES encryption in Virtex FPGAs using JBits,"in IEEE Symposium on Field-Programmable Custom ComputingMachines, Napa Valley,CA2000, pp. 113-121.

Miss, ChabukswarPunam Milind received his B.E. degree in Electronics & Communication Engineering in the Amrutvahini College of Engineering, SPPU Pune and pursuing M.E.VLSI and Embedded system from Sahyadri Valley College of Engineering and Technology, Rajuri, Pune, Maharashtra at Pune University. Her area of interest is VLSI System designs.

Prof. Mr. Manoj Kumar Singh completed his M.E (DC) and PhD(App.). He is currently an Asst. Professor and HOD of E&TC Department at Sahyadri Valley College of Engineering & Technology, Rajuri, Pune, Pune University, India. His current research intereset includes Image Processing & Digital Signal Processing.

Prof. Mr. Balramudu P. completed his M.E. and PhD (App.). He is currently an Asst. Professor and Vice principal atSahyadri Valley College of Engineering & Technology, Rajuri, Pune, Maharashtra in Pune University, India.