IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

Key Reconfiguration in Des Algorithm

Khemraj Deshmukh
khemraj.deshmukh@gmail.com

Prof. Vishal Moyal
vishalmoyal@gmail.com

Abstract — **A hardware design with the key reconfiguration is proposed based on the DES algorithm, and the FPGA implementation is presented in this paper. Based on the past results of the DES encryption algorithm implementation, due to the relativity between the generation of sub-key and the critical arithmetic key cracking of DES is easy, so the key can be reconfigured for security. Linear feedback shift register and chaos theory is used to provide reconfiguration facility to algorithm. Simulation and results shows the effectiveness of proposed work.**
Keywords —**DES, FPGA, Encryption.**

I. INTRODUCTION

Data Security is an important parameter for the industries. It can be achieved by Encryption algorithms which are used in the process called cryptography. It is a technique used to avoid an unauthorized access of data. It helps to provide accountability fairness and accuracy and also provide confidentiality. In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm.

The Data Encryption Standard (DES) [1] is a block cipher designed by a team from IBM in the 1970s, and later the algorithm was adopted as a federal standard by the U.S. National Bureau of Standards. The standard was used to provide a method for protecting sensitive commercial and unclassified data. After DES became a national standard in 1977, it was widely used to encrypt government and commercial data. Nowadays, DES is considered to be insecure for many applications because it has a short key size, which is only 56 bits. For example, in the DES Challenge III, which was one of the series of brute force attack contests organized by RSA Security, the secret key of DES was recovered in 22 hours 15 minutes in January 1999 [2]. The U.S. National Institute of Standards and Technology (NIST), which was previously known as the National Bureau of Standards, made a call for new algorithms to develop the Advanced Encryption Standard to replace DES in 1997.

Cryptography includes two basic components: Encryption algorithm and Keys.

If sender and recipient use the same key then it is known as symmetrical or private key cryptography. It is always suitable for long data streams. Such system is difficult to use in practice because the sender and receiver must know the key. It also requires sending the keys over a secure channel from sender to recipient [3]. The question is that if secure channel already exist then transmit the data over the same channel.

On the other hand, if different keys are used by sender and recipient then it is known as asymmetrical or public key cryptography. The key used for encryption is called the public key and the key used for decryption is called the private key. Such technique is used for short data streams and also requires more time to encrypt the data [3]. To encrypt a message, a public key can be used by anyone, but the owner having private key can only decrypt it. There is no need for a secure communication channel for the transmission of the encryption key. Asymmetric algorithms are slower than symmetric algorithms and asymmetric algorithms cannot be applied to variable-length streams of data.

Cryptography Techniques

There are two techniques used for data encryption and decryption, which are:

A. Symmetric Cryptography

If sender and recipient use the same key then it is known as symmetrical or private key cryptography. It is always suitable for long data streams. Such system is difficult to use in practice because the sender and receiver must know the key. It also requires sending the keys over a secure channel from sender to recipient. There are two methods that are used in symmetric key cryptography: block and stream. The block method divides a large data set into blocks (based on predefined size or the key size), encrypts each block separately and finally combines blocks to produce encrypted data. The stream method encrypts the data as a stream of bits without separating the data into blocks. The stream of bits from the data is encrypted sequentially using some of the results from the previous bit until all the bits in the data are encrypted as a whole.

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

B. Asymmetric Cryptography

If sender and recipient use different keys then it is known as asymmetrical or public key cryptography. The key used for encryption is called the public key and the key used for decryption is called the private key. Such technique is used for short data streams and also requires more time to encrypt the data. Asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because they require more computational processing power. To get the benefits of both methods, a hybrid technique is usually used. In this technique, asymmetric encryption is used to exchange the secret key; symmetric encryption is then used to transfer data between sender and receiver.

II. DES Algorithm

Data Encryption Standard (DES) is a cryptographic standard that was proposed as the algorithm for the secure and secret items in 1970 and was adopted as an American federal standard by National Bureau of Standards (NBS) in 1973. DES is a block cipher, which means that during the encryption process, the plaintext is broken into fixed length blocks and each block is encrypted at the same time. Basically it takes a 64 bit input plain text and a key of 64-bits (only 56 bits are used for conversion purpose and rest bits are used for parity checking) and produces a 64 bit cipher text by encryption and which can be decrypted again to get the message using the same key.

Additionally, we must highlight that there are four standardized modes of operation of DES: ECB (Electronic Codebook mode), CBC (Cipher Block Chaining mode), CFB (Cipher Feedback mode) and OFB (Output Feedback mode). The general depiction of DES encryption algorithm which consists of initial permutation of the 64 bit plain text and then goes through 16 rounds, where each round consists permutation and substitution of the text bit and the inputted key bit, and at last goes through an inverse initial permutation to get the 64 bit cipher text.

This paper presents a scheme to reconfigure the small 64 bit of DES to make DES a bit secure.

III. Sub-key Generation in DES

Sub-keys used in round operations are generated by key scheduling procedure. The 64 bit is first fed to permutation choice 1 box for parity drop, it results an output of 56 bit binary stream which is the original key.

PC-1

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

Figure 1: Permutation Choice-1

The two halves of this 56 bits are shifted by bit in round 1, 2, 9 and 16 and by 2 bits in other round by Left in encryption and Right in decryption. After this 56 bits are fed to permutation choice 2 which output a 48 bit binary stream which is a sub-key for a particular round.

PC-2

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Figure 2: Permutation Choice-2

This is fed to round function for encryption and decryption. All sub-keys are dependent of the main key thus if someone know the key can easily decrypt the cipher.

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

IV. KEY RECONFIGURATION

Since the security of DES depends on the key protection, we are presenting a key reconfiguration to make des a bit secure.

Linear Feedback Shift Register

An LFSR is a shift register that, when clocked, advances the signal through the register from one bit to the next most-significant bit. In other words, LFSR is a shift register whose input bit is a linear function of its previous state. For a general reference on the subject of LFSRs and related sequence generators. The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle.

So, we first fed 64 bit key to LFSR than for a time while it would shifted and will get an 64 bit output which will be a new key for des module for encryption and decryption.

Chaos Logistic Block

Due to the chaotic system has broad spectrum, class of stochastic characteristics, extreme sensitivity to structure parameter and initial state, and other properties, it has become an important branch of cryptography.

With a slight change in initial condition out for chaos block changes widely thus using initial parameters every time we can make change output of chaos block. New is to be generated by XORing the original key with chaos bit stream.

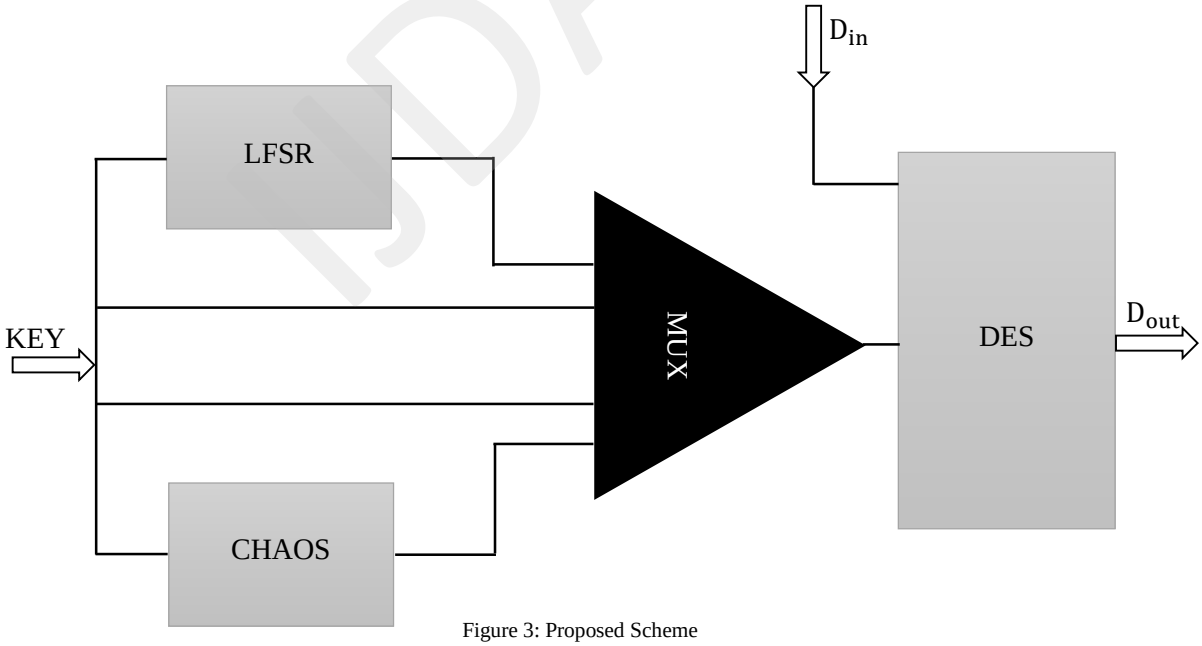

Figure 3: Proposed Scheme

By the above two discussions we have three key at same time for encryption. By selecting one at a time we can make des a bit secure such that to decrypt cipher not only the key needed but the knowledge of reconfiguration also mandatory.

IV. SIMULATION RESULT

Simulation of above algorithm is done in VHDL using Modelsim and Xilinx ISE. Key first fed to LFSR and Logistic block and the generated new key

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

will be selected by 4:1 mux and then new key will be given to DES for encryption.

For the test here we taking plaintext is AAAAAAAAAAAAAAAA and encrypting this using key F8F8F8F8F8F8F8F8 with select line of mux 10 that is chaos logic block in action, the cipher output is D18B044AEABAE288. Decrypting this cipher by with knowledge of scheme of reconfiguration is not possible.

Figure 4 and 5 below showing encryption and decryption by proposed scheme

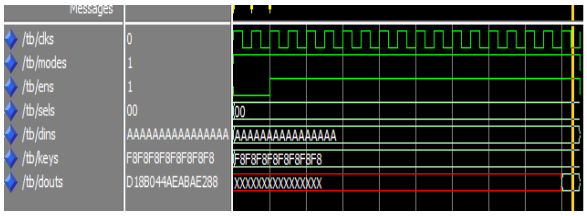

Figure 4: Encryption

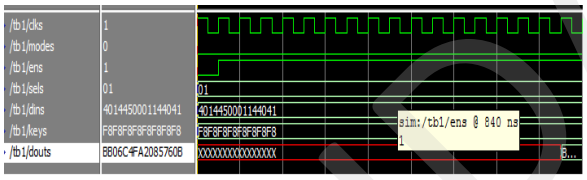

Figure 5: Decryption

Figure below shows the FPGA RTL Schematic of proposed scheme:

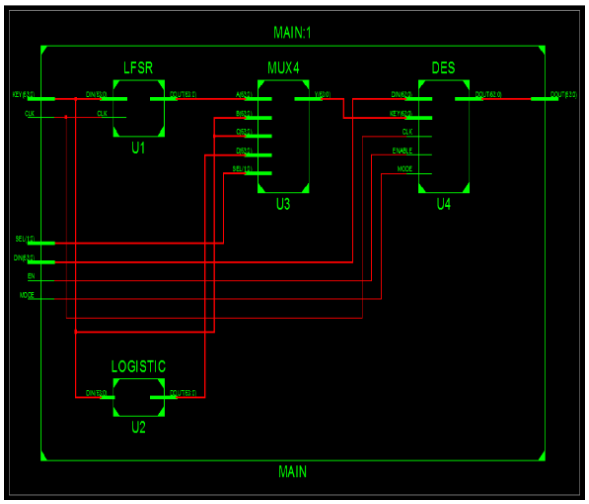

Figure 6: RTL View of Proposed Scheme

V. CONCLUSION

This paper proposed a scheme to reconfigure the key so that for any unauthorized party it will be very difficult to decrypt the cipher without knowing the scheme of encryption. This paper is FPGA encryption of proposed scheme that needs to be check with real world data. The future work can be the implementation and compatibility with existing hardware.

REFERENCES

[1]. National Bureau of Standards, Data Encryption Standard (DES), US Department of Commerce. Federal Information Processing Standards Publication 46 (FIPS PUB 46), 15 January 1977.

[2]. RSA Security. RSA's DES Challenge III is solved in record time. Available at: http://www.rsa.com/rsalabs/node.asp?id=2108, 18 January 1999.

[3]. Seung-Jo Han, "The Improved Data Encryption Standard (DES) Algorithm" 1996, pp 1310-1314.

[4]. Kaicheng Lu, "Computer Cryptography (third edition)", tsinghua university press, Beijing, 2003.

[5]. Li Jiang, Weixiong Jin, "Chaotic Encryption Technology and Its Algorithm", Journal of Huaihai Institute , vol. 13(4), 2004, pp. 39^12.

[6]. Jinhu Lv, Junan Lu, Shihua Chen, "Chaos Time Series Analysis And Its Application",Wuhan University Press, Wuhan, 2002.

[7]. HuaQing Software Embedded Training Center, "FPGA Application Development Introductory With Typical Examples," People's Telecon Publishing House, beijing, 2008.

[8]. Patterson, C. (Xilinx Inc.), "High performance DES encryption invirtex FPGAs using Jbits" Proc. IEEE Symp. on Field programmable custom computing machines, FCCM '00, Napa Valley, CA, USA,Apnl 2000 (IEEE Comput. Soc, CA, USA, 2000), pp. 113-121

[9]. M.L. Akkar, C. Giraud, "An Implementation of DES and AES Secure againts Some Attacks", in the proceedings of CHES 2001, Lecture Notes in Computer Sciences, vol 2162, pp 309-318, Paris, France, May 2001.

[10]. Ji Yaoa, Hongbo Kang, "FPGA Implementation of Dynamic Key Management for DES Encryption Algorithm", 2011.

[11]. Adleman, Leonard M. (June 10–12). "On Applying Molecular Computation to the Data Encryption Standard". Princeton University.

[12]. Cracking DES — Secrets of Encryption Research, Wiretap Politics & Chip Design. Electronic Frontier Foundation. ISBN 1-56592-520-3.

[13]. Burnett, Mark; Foster, James C. (2004). Hacking the Code: ASP.NET Web Application Security. Syngress. ISBN 1-932266-65-8.

[14]. Diffie, W.; Hellman, M.E. (1977). "Exhaustive Cryptanalysis of the NBS Data Encryption Standard". Computer 10.