Volume 4, Issue 12, December 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Dynamic Key Generattion to Enhance DES Algorithm Securities Using FPGA

Akhilesh Gautam, Prof. Preet Jain
Department of ECE, SVITS, Indore,
Madhaya Pradesh, India

Abstract— This paper proposed a "Dynamic key generation" for DES algorithm which makes DES strong. DES is acronym for "Data Encryption Standard". Based on the analysis of DES algorithm, the generation of sub key and its arithmetic is weak, so that key generation can be reconfigured. For key generation, we can use three modes, first one is "Direct key" by the user, second one is key shifted through "LFSR", and third one is key generated by "chaotic or logistics" encryption.

For implementation this project, I have divided this into two part, first part is DES algorithm part another is key generation part. A control unit also initiate here to control round of DES and encryption/decryption mode.

Keywords— DES, Dynamic Key Generator, FPGA, LFSR, Chaotic Encryption.

I. INTRODUCTION

Cryptography or secret writing means scrambling a message or creating a digest of the message. In other words cryptography may be defined as the science and art of transforming message to make them secure and immune to attacks. DES is one of the best known cryptographic algorithms, and has been used since when it introduces in 1976 and is still used today despite the fact that it doesn't offer a sufficient level of security [1].

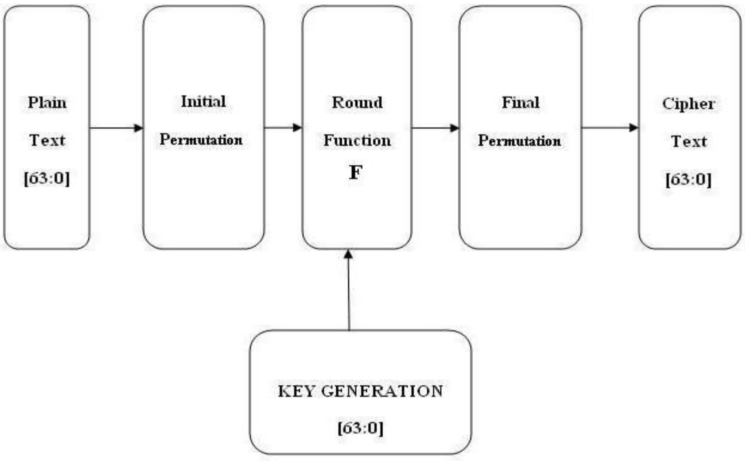
The DES algorithm is a block cipher that uses the same binary key both to encrypt and decrypt data blocks, and thus is called a symmetric key cipher. DES operates on 64-bit "plaintext" data blocks, processing them under the control of a 64-bit key to produce 64 bits of encrypted cipher text. Similarly, the DES decryption process cipher text block using the same 64-bit key to produce the original 64-bit plaintext block.

The main weakness of DES algorithm is its key generation. According to kerckhoff's principle, predicting the key should be so difficult that there is no need to hide the encryption/decryption algorithms. In this paper we proposed a dynamic key generation unit to enhance security of DES algorithm using FPGA.

II. ALGORITHM DESCRIPTION

A. Data Encryption Standard algorithm Theory

DES is one of block encryption algorithm of mathematical algorithms for the computer data encryption protection. DES is a symmetric (Private Key) algorithm. A block diagram of DES is shown in ***Fig. 1.1***.



BLOCK DIAGRAM OF DES ALGORITHM

Fig. 1.1

It is a block cipher operating on 64-bit blocks of plaintext utilizing a 64-bit key. The original 64-bit plaint text is rearranged by the initial permutation. After an initial permutation, the 64-bit input is divided into two equal parts. First is Right half (R_0) and second is left half (L_0), each 32 bits in length.

DES has 16 rounds. In each round, a function **F** is performed. ***Fig.1.2*** describe Round function of DES algorithm. As shown in figure fig.1.2, the 32-bit right half of the plaintext $\boldsymbol{R_{i-1}}$ is expanded to 48-bits by expansion permutation block and then XORed with a 48-bit sub-key $\boldsymbol{K_i}$.

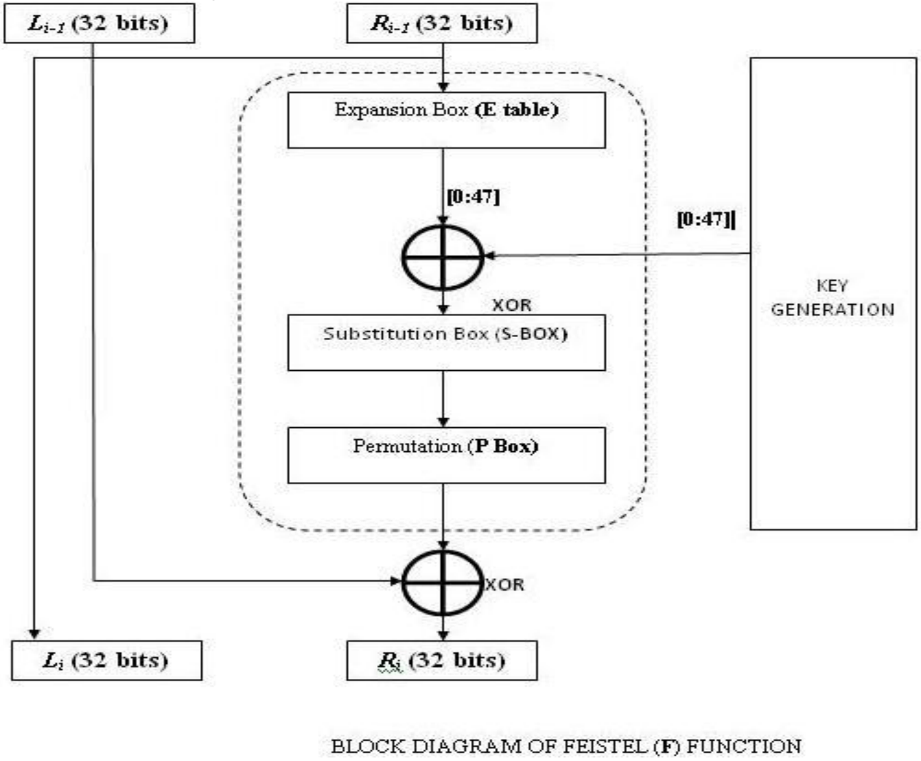


Fig. 1.2

The result is then fed into eight substitution boxes (**S**-boxes), which transforms the 48-bit input to a 32-bit output. Finally, a straight permutation (**P**-permutation) is performed, the output of which is XORed with the left half $\boldsymbol{L_{i-1}}$ to obtain the new right half $\boldsymbol{R_i}$. The right half $\boldsymbol{R_{i-1}}$ becomes the new left half $\boldsymbol{L_i}$ ***[3]***.

The S-box is the critical part of the DES algorithm. It realizes the non-linear transformations.

In Fig. 1.1, it shows that key generator is independent of DES algorithm computation, which offers the potential and convenience for key configuration. The First step of key generation is to remove the parity check bits in the 64-bit key. Every eighth bit is used for parity checking, leaving 56-bits. The parity bits are 8, 16, 24, 32, 40, 48, 56 and 64 bit. Now a different 48-bit sub-key is generated for each of the 16 rounds of DES. The sub keys are determined by dividing the 56-bits into two 28-bit lengths of data. Then both halves are shifted left by either one or two bits depending on the round number.

In rounds 1, 2, 9 and 16 of the DES algorithm the halves are shifted one position to the left and for all other rounds two positions to the left.

B. Linear Feedback Shift Register

LFSR is an acronym for Linear Feedback Shift Register. Due to LFSR is easy to constructed and implemented by software and hardware, so that it can be used to as a Good key Stream generator. A LFSR consists a shift register and a linear feedback function of its previous states. As shown in ***Fig. 1.3***.

The shift register is sequence of M flip flops, $\mathbf{B_M}$ to $\mathbf{B_{M-1}}$, where **e**ach flip flop holds a single bit. The flip flops are initialized to an M-bit word called the **Seed.** As shown in Fig 1.3, $\mathbf{B_M}$ is a linear function of $\mathbf{B_0}$, $\mathbf{B_1}$, $\mathbf{B_2}$,**…**,$\mathbf{B_{M-1}}$ *[1]*.

Shift register can be divided according to its type of inputs and outputs. For example serial inputs and parallel outputs or parallel inputs and serial inputs.

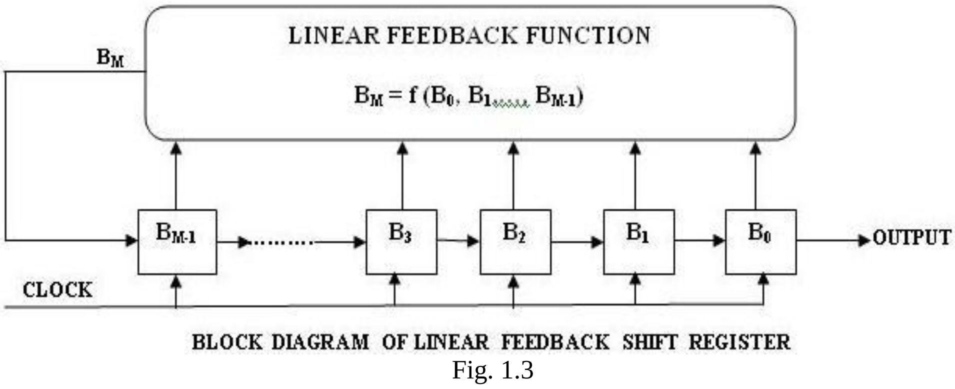

LINEAR FEEDBACK FUNCTION
$B_M = f(B_0, B_1, \ldots, B_{M-1})$
B_M
B_{M-1}
B_3
B_2
B_1
B_0
OUTPUT
CLOCK
BLOCK DIAGRAM OF LINEAR FEEDBACK SHIFT REGISTER

Fig. 1.3

LFSR has broad area of applications. The main domain of LFSR applications include generating pseudo-random numbers, pseudo-noise sequences, fast digital counters and whitening sequences *[7]*.

C. Chaotic Encryption.

In recent years, chaotic systems are more researched in the field of key generation of cryptography. In general, “chaos” means “a state of disorder”. However, in chaos theory means a nonlinear dynamic behaviour of the law control.

For a dynamical system to be classified as chaotic, it must have the following properties:

- It must be sensitive to initial conditions;
- It must be iterative unrepeatability

One-dimensional Logistic map is a very simple chaotic map from the point view of mathematical form. But this system has an extremely complex dynamics, wide applications in the field of secure communication, so that the Logistic map can be used for “Dynamic key generation unit” *[4]*.

Logistic model is one of the chaotic models; its equation is as follows:

$$Y_{N+1} = \mu \times Y_N \left(1 - Y_N\right) \qquad (1)$$

Where (N = 0, 1, 2…), and the initial value $Y_N \in (0,1)$.

The research of chaotic dynamical systems points out that the logistic map gradually reaches to chaos from times bifurcation phenomena when $3 \leq \mu \leq 4$. That is, {Y_N, N=1,2,3,…}, which is produced by Logistic map. It is non-periodic and convergence under initial condition.

In theory chaotic sequence is not pseudo-random, but truly stochastic, so key generator with high intension can be constructed using these characteristics *[2]*.

III. MOTIVATION AND OBJECTIVE

My motivation originated from studying the DES algorithm, and its insecurities.

The main weakness of DES algorithm is it’s 56-bit key. Using 56- bit key, there are 2^{56} possible keys available, now a day which are easily crack by “brute force attacks”. “Brute-force” means in which involves trying all 2^{56} keys. Apart from this out of 2^{56} keys, 4 are weak key, 12 are semi weak and 48 are possible weak key [1].

If we increase number of possible key generation way more than 2^{56}, then we can enhance security in DES.

To increase number of ways of key generation more than 2^{56} , we can use three mode of key generation which are;

- Key generation through Linear Feedback Shift Register (LFSR).
- Key generation using chaotic encryption.
- Direct key generation by user.

For example if a user generates a key for DES, he has 2^{56} ways but after key shifted through LFSR there are also 2^{56} ways available (depending upon feedback function), so that finally user has 2^{112} way.

For make more confusion in key generation, the key can be generated by any of the above methods.

IV. THE PROPOSED DESIGN

In order to enhance the security of DES algorithm, this PAPER presents the dynamic key configuration to improve DES algorithm, As shown in figure ***4.1*** with Linear Feedback Shift Register (LFSR) and the chaotic (logistic) encryption can increasing the complexity of the original keys.

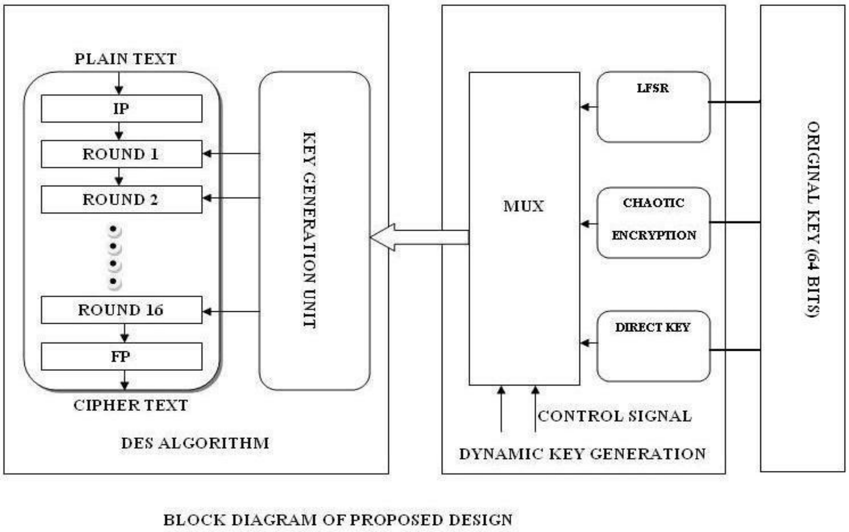


Fig. 4.1

The 64-bit original key can be configured based on the controlled signals. It either directly introduces the initial key to participate in DES encryption algorithm or passes it through a LFSR or a chaotic encryption, and then gets a new key stream to participate in DES to enhance the security of the key of DES algorithm.

V. CONCLUSIONS AND FUTURE WORK

Data Encryption Standard algorithm is a type of symmetric-key encipherment algorithms. Symmetric-key encryption is a type of cryptosystem in which encryption and decryption are performed using a single (secret) key. As we can see, secret key play a very important role in DES security, so that a good key generation unit required. Using Dynamic key generator, the generated key has characteristics of unpredictability and unrepeatability. Using this approach the dynamic key generator can achieve the high speed and can be reduce logic complexity.

Using proposed design, a general purpose IC can be designed for DES algorithm with high secrecy of the key in real time data communication. This design has a broad application area in field of data communication, and secure data transmission.

REFERENCES

[1] Behrouz A. Forouzan, “Cryptography and Network Security”, Special Indian Edition., TMH: New Delhi, 2007.

[2] Chen Zhuo, Zhang zhengwen, Jiang Nan, “A Session Key Generator Based on Chaotic Sequence.” International Conference on Computer Science and Software Engineering, 2008, DOI 10.1109/CSSE.2008.833.

[3] William Stallings, “Cryptography and Network Security-Principles Practice”, Fifth Edition, Prentice Hall, 2006.

[4] Ji Yao, Hongbo Kang, “FPGA Implementation of Dynamic Key Management for DES Algorithm” International Conference on Electronics & Mechanical Engineering and Information Technology, Dated 12-14 Aug 2011.

[5] Sivaprakasam S and Shore K A, “Message encoding and Decoding using chaotic external-cavity diode lasers,” IEEE Journal of Quantum Electronics, 2000, 36(1):35-39.

[6] Ke Wang, “An encrypt and decrypt algorithm Implementation on FPGAs”, 2009 Fifth International Conference on Semantics, Knowledge and Grid, DOI 10.1109/SKG.2009.74.

[7] Amit Kumar Panda, Praveena Rajput, Bhawna Shukla, “FPGA Implementation of 8, 16 and 32 Bit LFSR with Maximum Length Feedback Polynomial using VHDL”, 2012 International Conference on Communication Systems And Network Technologies, DOI 10.1109/CSNT.2012.168.