Efficient key management methods for symmetric cryptographic algorithm

Sreehari K N
Dept.of Electronics and communication engineering
Amrita VishwaVidyapeetham,Amritapuri,India
sreehari.kn86@gmail.com

Abstract: key management is major issue in cryptographic algorithms. Key management includes key generation and sharing of secret key between sender and the receiver. The generated key should be random in nature. The sharing of key through secure channel is also a major research area. In this paper, different key generation methods are considered for a symmetric algorithm. In the first method, lfsr based key is used. In the second method, hash function method is used for key generation. The cryptographic system with above key generation techniques is modelled using hardware description language using VIVADO software

Keywords: DES, hash function, LFSR, encryption

I.INTRODUCTION

Key generation and key sharing through secure channel is a major research area in cryptographic field. Different key generation methods are already available. In this paper, key for symmetric cryptographic algorithm is generated using different methods. Different key generation methods are used so that it is difficult to for the attacker to decrypt the cipher text easily

Data encryption standard algorithm is chosen as example for symmetric algorithm. Basic DES algorithm is not good to resist different channel attacks[3]. So in this paper, double DES is considered which encrypts the the message using two keys.

Linear feedback shift register(LFSR) can be used to generate random numbers. The output of linear feedback shift register can be given as two keys for double DES algorithm.64 bit random sequence key can be generated using LFSR.

The hash function method can also be used to generate key for symmetric algorithm. The output of hash function is a fixed length sequence for a given message. MD5 hash algorithm can be used for generating fixed length sequence. The output of MD5 algorithm which is of size 128bit can be used as key for double-DES algorithm.

II.LITERATURE REVIEW

A. Key generation using LFSR

Random number generator can be implemented in hardware. The numbers generated can be either true random or pseudo random. The next state of true random sequence is not predictable, but in pseudo random numbers it is predictable[6],[7],[8].

In this paper, a LFSR with four shift register flipflops implemented. The output of LFSR is given as key for data encryption standard algorithm. The basic structure of linear feedback register is shown in below figure 1

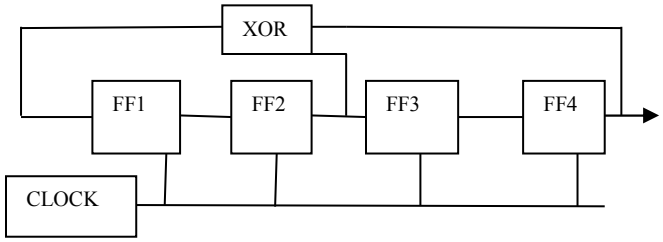

Fig 1: basic LFSR structure

An n-stage LFSR with a initial seed value will generate $2^{\wedge n}$-1 random numbers. A 4 bit LFSR is used to generate the key for DES encryption [9],[10]. A four bit LFSR with a given seed value will generate 15 sequences. We can generate 64 bit key from it. A four bit LFSR with a primitive polynomial as characteristic polynomial is chosen for random sequence generation. The LFSR structure used in this work is shown below in figure 2. The primitive characteristic polynomial used to get the sequence is

$$f(x) = x4 + x3 + 1$$

The seed value of LFSR is determined from four least significant bits of original 64 bit key. Two keys are generated using this method for double-DES operation.

978-1-5386-1508-9/18/$31.00 ©2018 IEEE

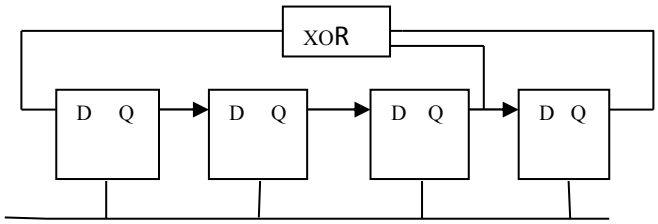

Fig 2. Four bit linear feedback register

B. Key Generation using Hash function

Hash function algorithms produces fixed length bit sequence independent of the input message size[5]. The fixed length sequence can be used as key for double DES. Since hash function output is not easily reversible, it is good for security. In this work, MD5 hash algorithm is used whose 128 bit sequence used as key 1 and key 2 of double DES. The input to MD5 algorithm is original 64 bit key. The structure of one round in MD5 algorithm is shown below in figure 3. First step is the conversion of original message to a block of 512 bits. Registers of size 32 bits(A, B, C ,D) are used to store intermediate result and final result. The operations like logical and,or,xor, modular addition, shifting are performed in each round of operation.

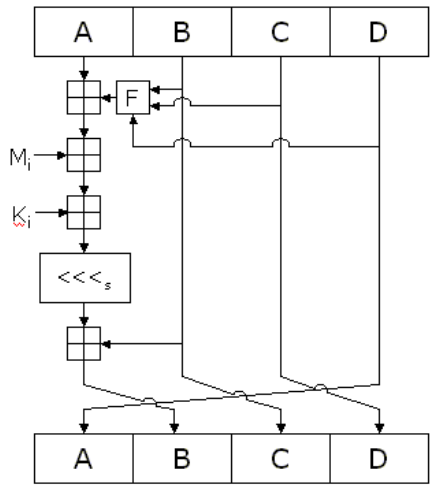

Fig 3. Basic MD5 algorithm

C. Double-DES algorithm

DES algorithm is a block cipher algorithm which uses message block of size 64 bit and key of size 64 bit[1][2]. The normal DES algorithm is vulnerable to different attacks. Double DES algorithm is used for increasing the security. Double DES algorithm performs the encryption of message twice with two different keys to increase the security[4]. Basic DES functional diagram is shown in figure 4 and double-DES block diagram is shown in figure 5

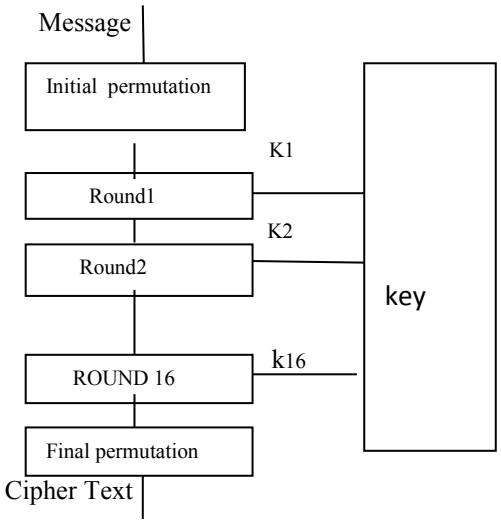

Fig 4. Basic DES encryption structure

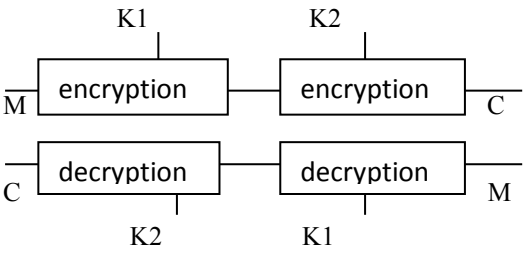

Fig 5.Double-DES encryption and decryption

D. Encryption and Decryption using different keys

The original key size is 64 bit. When the select line is 0, key to DES block is taken from LFSR output. The LSB four bits are initially taken and given as seed to LFSR.LFSR produces random bit sequence and this value is chosen as key1. The MSB four bits are then chosen as the next seed of LFSR which again produces random sequence and it can be used as key 2

When the select line is 1, the key to DES block is taken from hash function output. The 64 bit normal key is the input to MD5 algorithm and the output is 128 bit. 128 bit out is used as key1 and key 2(64 bit each) for double DES-algorithm The figure 6 shows complete hardware architecture for the encryption and decryption

In the receiver side, the same two methods are used to generate key for decryption. The LFSR will generate two keys from the original key. The MD5 will also generate 128 bit from original key which can be used as key for decryption. The encryption and decryption is not using the original key. A new key is generated from original key using two methods, so it is difficult for the attacker to get the actual key used for encryption.

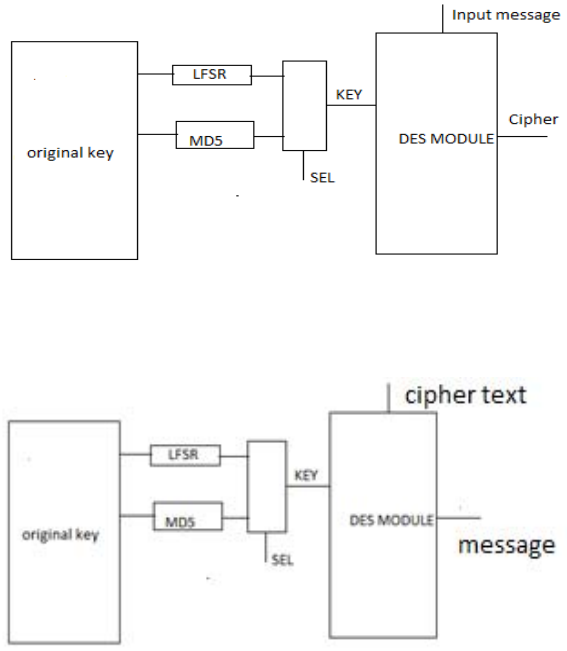

Fig 6: Encryption and decryption

III.EXPERIMENTS AND RESULTS

The system is modelled using verilog description language and functional simulation is carried out using vivado software [9]. The functional simulation is carried out with lfsr based key system and hash function based key system

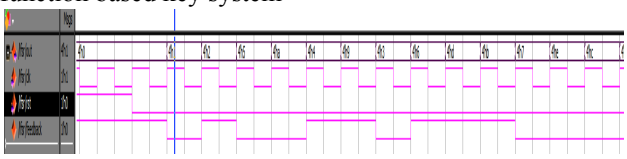

Fig 7.LFSR simulation

The above simulation shows the output of a 4 bit LFSR. The seed value for the LFSR is taken from the original key. RTL schematics of LFSR is shown in figure 8

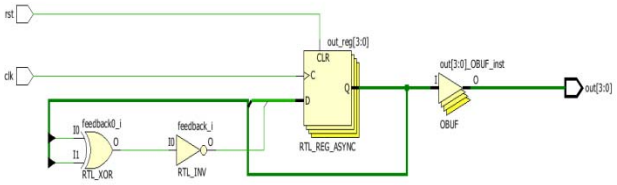

Fig 8.RTL schematics of LFSR

The simulation waveform (fig9) shows 128 bit output of the MD5 algorithm. The input to MD5 algorithm is normal 64 bit key. This output can be used as keys for des algorithm

Fig 9.MD5 hash function output

The simulation waveform (fig 10 and fig11) shows the encrypted output of the DES module with key from LFSR and hash function respectively

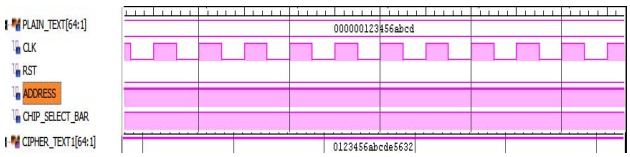

Fig 10: Simulation of encryption using key generated using hash function

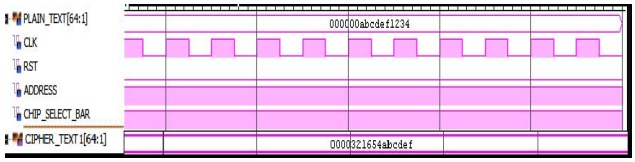

Fig 11.Simulation of key using key generated using hash functions.

IV.CONCLUSION AND FUTURE WORK

Original key for double-DES algorithm is modified using LFSR technique and hash function technique. The cryptosystem can choose either the output from LFSR as key for encryption or hash function output as a key for encryption. In the receiver side,the same methods can be used to generate key for decryption This methods will make difficult for attacker to get original data from cipher text, so it will increase the security.

As a future work, more methods can be adopted to increase the random nature of LFSR. The seed value can be generated using physically unclonable function

REFERENCES

1. Mohamad Noura, Hassan N. Noura, Ali Chehab, Mohammad M. Mansour, and Raphaël Couturier, "S-DES: An Efficient & Secure DES Variant", 2018 IEEE Middle East and North Africa Communications Conference

2. M. McLoone,J.V. McCanny, "High-performance FPGA implementation of DESusing a novel method for implementing the key Schedule, IEE Proc.-Circuits Devices Syst., Vol. 150, No. 5, October 2003

3. Dr. Mohammed M. Alani, "DES96-Improved DES Security", 2010 7th International Multi-Conference on Systems, Signals and Devices.

4. Pranav M, ArchanaK Rajan, "DES security enhancement with dynamic permutation", 2015 International Conference on Applied and Theoretical Computing and Communication Technology

5. Keonwoo Kim, Un Sung Kyong, "Efficient Implementation of MD5 Algorithm in Password Recovery of a PDF file, 2012 7th International Conference on Computing and Convergence Technology

6. DebarshiDatta, BipaDatta, HimadriSekhar Dutta, "Design and Implementation of Multibit LFSR on FPGA to Generate Pseudorandom Sequence Number , 2017 Devices for Integrated Circuit (DevIC), 23-24 March, 2017, Kalyani, India.

7. Hong-Sik Kim and Sungho Kang, "Increasing Encoding Efficiency of LFSR Reseeding-Based Test compression", IEEE transactions on computer-aided design of integrated circuits and systems, vol. 25, no. 5, may 2006

8. ValarmathiMarudhai, "Implementation of LFSR on ASIC", 2012 Annual IEEE India Conference (INDICON)

9. Ramesh Bhakthavatchalu, Rekha, B. S., Divya, G. A., and Jyothi, V. U. S., "Design of AXI bus interface modules on FPGA", in Proceedings of 2016 International Conference on Advanced Communication Control and Computing Technologies, ICACCCT 2016, 2016, pp. 141-146

10. 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