FPGA BASED NETWORK SECURITY USING RC5 ALGORITHM

Prof.S.C. Wagaj[1], Warake Snehal S.[2], Harer Arti L.[3], Solpure Pooja R.[4]

[1,2,3,4] *Professor, RSCOE, Pune, (India)*

ABSTRACT

In day to day life communication is very important aspect. Secure transmission of data from one place to another place is necessary to protect data from hackers & attackers. This paper presents FPGA based efficient & secure data transmission for communication system. RC5 is a symmetric block cipher that is the same secret cryptographic key is used for both encryption & decryption. RC5 is suitable for hardware & software, has variable number of rounds, variable length cryptographic key, simple & low memory requirement. It is described with VHDL & implemented on FPGA (SPARTEN 3E).

Keywords- Rc5, Symmetric Encryption & Decryption, Block Cipher, VHDL, FPGA (SPARTEN 3e)

I. INTRODUCTION

In this paper we present RC5 algorithm for secure data transmission.**RC5** is a block cipher notable for its simplicity & designed by Ronald Rivest. RC stands for Rivest Cipher or alternatively Ron's code. With the development of communication and network technology, many applications take security into consideration.

RC5 is parameterized algorithm and a particular RC5 algorithm designated as RC5-w/r/b. We summarized these parameters below,

w = The word size, in bit. Standard value is 32 bit; allowable values are 16,32,64. RC5 encrypts two word blocks so that the plain text and cipher text blocks are each 2w bits long.

r = r is the number of rounds. Allowable values are 0,1,…….255.

b = The number of byte in secret key. Allowable values are 0,1,…….255.

In this paper we use 3 algorithms for RC5 implementation :

1. Key expansion algorithm
2. Encryption algorithm
3. Decryption algorithm

II. EXISTING SYSTEM

RC4 designed in 1987 by RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) . RC4 is most widely used stream cipher in software application. RC4 has a secret internal state which is permutation of all the N= 2^n possible n bits words, along with two indices in it. It is based on key scheduling algorithm and pseudo random generator algorithm. RC4 fails the standards set by cryptographers for a secure cipher in many ways, and it is not recommended for use in new application as there are a lot of methods of attacking RC4.Thus we implement RC5 algorithm.

III. PROPOSED SYSTEM

Below Fig. shows the block diagram of RC5 algorithm

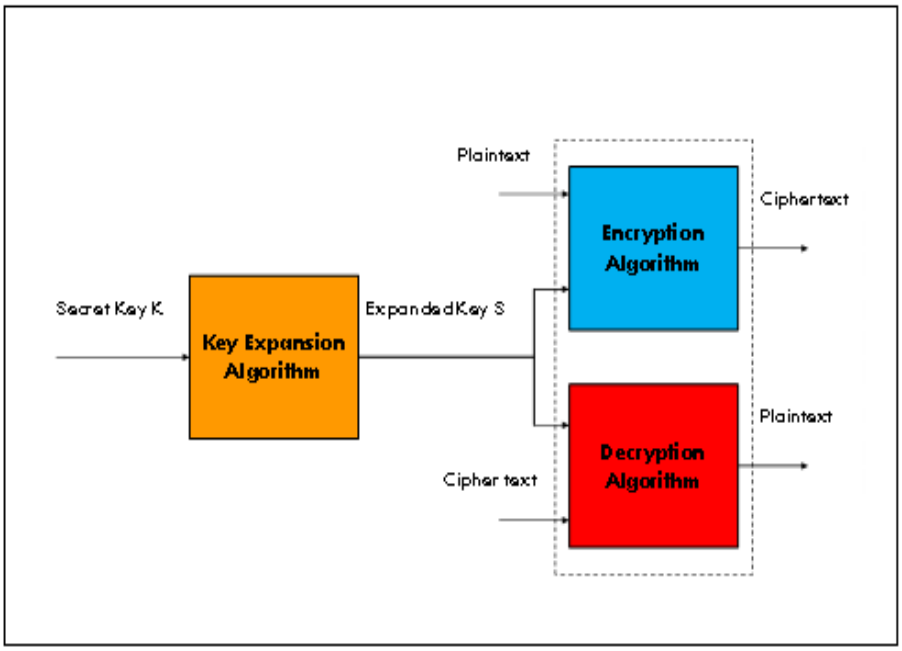


Fig.3.1 Block Diagram of RC5 Algorithm

3.1 Key Expansion Algorithm

RC5 performs some operations on the secret key to generate a total of t sub keys, which are stored in S array, S[0],S[1], …, S[t-1].

The key expansion algorithm consists of two constants (Magic numbers) and three simple algorithm parts

Step-1: Convert secret key bytes to words

Step-2: Initialize sub key array S (S[0], S[1], …, S[t-1])

Step-3: Mix the secret key into sub key array S

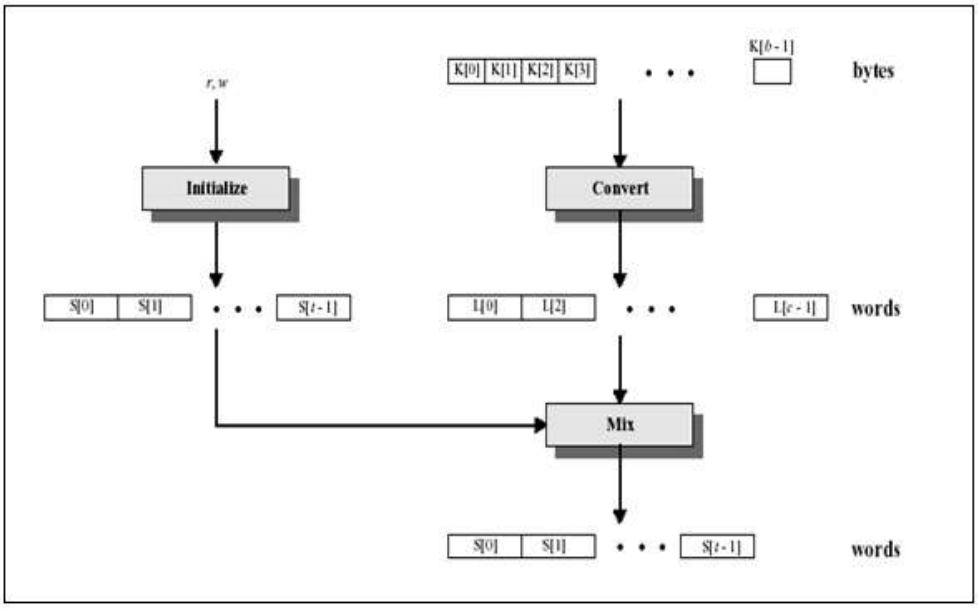


Fig3.2 Key Expansion Algorithm

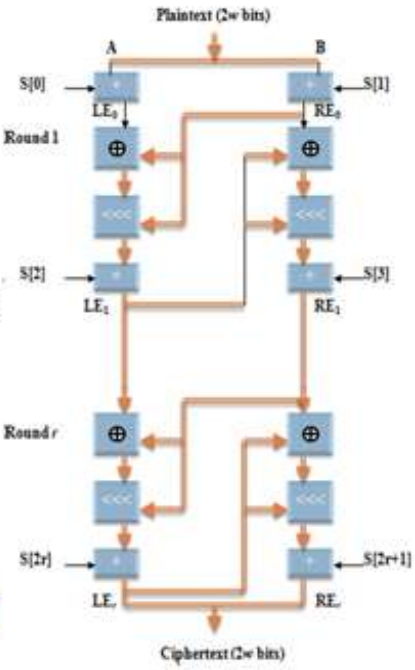
3.2 Encryption Algorithm

```
A = A + S[0];
B = B + S[1];

for i = 1 to r do
    A = ((A ⊕ B) <<< B) + S[2*i];
    B = ((B ⊕ A) <<< A) + S[2*i + 1];
```

A <<< B

Bits in A are rotated to left by the amount specified by lower log2(*w*) *bits in B*



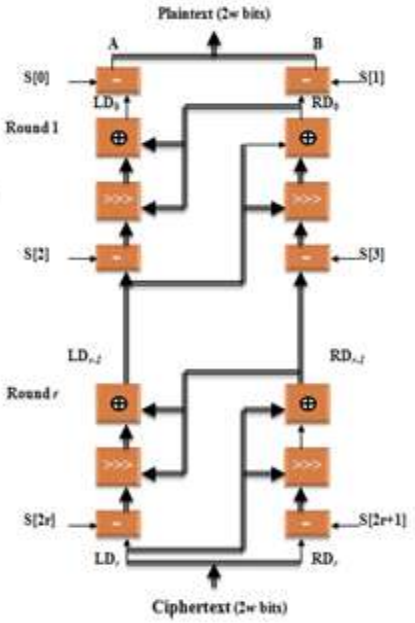
3.3 Decryption Algorithm

```
for i = r downto 1 do
    B = ((B - S[2*i +1]) >>> A) ⊕A;
    A = ((A - S[2*i]) >>> B) ⊕B;

B = B - S[1];
A = A - S[0];
```

A >>> B

Bits in A are rotated to right by the amount specified by lower log2(*w*) *bits in B*



IV. FEATURES

4.1 Symmetric block cipher (Like Feistel Network Structure)

The same secret cryptographic key is used for encryption and decryption.

4.2 Suitable for hardware and software

It uses only computational primitive operations commonly found on microprocessors.

4.3 Adaptable To Processors of Different Word

For example with 64 bit processor RC5 can exploit their longer work length. Therefore the number *w* of bits in a word is a parameter of RC5, different choices of this parameter results different algorithms.

4.4 Variable Number of Rounds

The user can explicitly manipulate the trade-off between higher speed and higher security. So the number of rounds *i* is a second parameter of RC5.

4.5 Variable Length Cryptographic Key

The user can choose the level of security appropriate for his application the key length *b* In bytes is thus a third parameter of RC5

V. APPLICATIONS

A. In military application
B. In medical application
C. In banking system

VI. FUTURE SCOPE

Here we trying to implement FPGA based network security using RC5 algorithm. The RC5 had requirements of low power, low delay, Variable length cryptographic key, Low memory& Variable number of rounds. The encryption and decryption process can be implemented in pipeline format to increase throughput. The RC5 Provides good security.

VII. CONCLUSIONS

In this paper we represents RC5 algorithm for network security application. Thus by using RC5 algorithm the data security may increased with some extend because of various operations are used for implementation of algorithm. The proposed design is described with VHDL & synthesized by Xilinx (SPARTEN 3E).

REFERENCES

[1] R.L. Rivest, "The RC5 encryption algorithm,"Proceedings of the 1994 Leuven Workshop on Fast Software Encryption,pp.86-96,Springer-Verlag,1995.
[2] V Chaitanya Tummalapalli, MD.Khwaja Minnuddin Chisti ,"implementation of low power RC5 algorithm in Xilinx FPGA",Vol.2, Issue 3,May-June 2012,pp.924-928.
[3] R.L.Rivest, "the RC5 encryption algorithm" ,proceeding Of the 1994 Leuven workshop on fast software encryption,pp.86-96,Springer-verilog,1995.
[4] Jing Liang, Qin Wang, Yue Qi, Feng Yu, "An area optimized implementation of
[5] Cryptographic algorithm RC5", Department of Computer Science and Technology Beijing, China.
[6] Girish Kumar B, Prabhu V2, Siva Prasad T, Ruban Thomas," Design and Implementation of FPGA
[7] Based Efficient Data Transmission Using Verilog", volume 3, Issue 11, November 2013.