

Hardware Implementation of Modified RC4 Stream Cipher Using FPGA

Jaya Dofe¹, Manish Patil²

Dept. of Electronics, PG Student Maharashtra Academy of Engineering, Alandi, Pune University of Pune

Abstract: — In this project work, an efficient hardware Implementation of modified RC4 stream-cipher is proposed. In contrary to previous design, which requires four memories each of size 256 X 8, the proposed system can be implemented by using only two memories each of size 128 X 7. Due to the reduction in the memory size the strength of encryption can be increased. Design of RC4 stream cipher for data Security; RC4 uses a variable length key from 1 to 128 bytes to initialize a 128-byte array. The array is used for subsequent generation of pseudo-random bytes and then generates a pseudorandom stream, which is XORed with the plaintext/cipher text to give the cipher text/plaintext. The RC4 stream cipher works in two phases. The key setup phase and the pseudorandom key stream generator phase. Both phases must be performed for every new key. Below is the brief about Security functions carried out at Security Layer. The RC4 algorithm will be implemented by FPGA using VHDL software platform.

Keywords: — RC4, Stream cipher, KRAM, SRAM, Data Serializer, K Stream Serializer.

I. INTRODUCTION

Message secrecy is one of most important aspect of communication but especially in wireless environment messages are highly insecure and encryption is must in such environment. The various encryption algorithms are available but RC4 encryption algorithm is stream type and can be implemented in hardware and software.

The RC4 stream cipher is implemented in hardware by P. Kitsos, G. Kostopoulos, N. Sklavos, and O. Koufopavlou VLSI Design Laboratory, Electrical and Computer Engineering Department, University of Patras, Patras, Greece . The same hardware implementation is fast and reliable as compared to software implementations and block ciphers algorithms. RC4 is used for encryption in the wired equivalent privacy (WEP) protocol (part of the IEEE 802.11b wireless LAN security standard), IEEE 802.11 i Lotus Notes, Apple computer's AOCe and Oracle secure SQL. The IEEE 802.11 i uses the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Page Layout

Standard (AES). TKIP uses the RC4 stream cipher as the encryption and decryption algorithm and all involved parties must share the same secret key.

RC4 algorithm strengths

- [1] It uses stream cipher and it can cipher individual units (perhaps bits or bytes) as they occur. It can (but may choose not to) cipher individual data elements immediately, as they arrive. This is a stream cipher signature, and can be identified by analysis of the design. So it takes less time to generate the cipher text.
- [2] RC4 algorithm uses stream cipher that is often used in application where plaintext comes in quantities of unknowable length. Does not need to fill a block, so does not need block padding, and does not need a padding removal structure.
- [3] A particular RC4 algorithm key can be used only once. Encryption is faster than the other algorithms that uses block cipher. The chance of losing the data in wireless transmission is very high, but RC4 algorithm can easily synchronize with the transmission even if the data is lost.
- [4] RC4 algorithm is implemented in software, so the complexity is less and it is cheaper as the software can be easily changed according to the requirements.

II. METHODOLOGY

Typical stream cipher is shown in figure (1), in which the first block indicates encryption phase and second block indicates decryption phase. The sender encrypts plain text with key stream, which is generated by the key stream generator with the privacy key i.e. distributed on secure channel. On the other hand, the receiver decrypts the received the cipher text with key stream which is generated by the key stream generator with the privacy key i.e. also distributed on secure channel.



Fig1. Block diagram of stream cipher

Figure 1 shows the block diagram of proposed modified RC4 algorithm which uses a variable key length from 1 to 128 bytes to initialize a 128 byte array. The array is used for subsequent generation of pseudo-random bytes and then generates a pseudorandom stream, which is XORed with the plaintext / cipher text to give the cipher text / plaintext.

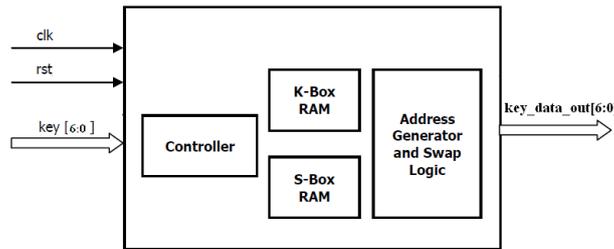


Fig 2. Block diagram of modified RC4 cipher

There are 128-byte arrays, S-Box and K-Box. The S-array is filled linearly such as $S_0=0, S_1=1, S_2=2, \dots, S_{127}=127$.

The K-array consists of the key, repeating as necessary times, in order to fill the array. The RC4 stream cipher works in two phases. The key setup phase and pseudorandom key stream generator phase. Both phases must be performed for every new key.

```

Key setup phase:
For i = 0 to 127
  J = (j + S(i) + K(i))
  Swap S (i) and S (j).
    
```

Fig 3 (a). Key Setup Phase

There are 128-byte arrays, S-Box and K-Box. The S-array is filled linearly such as $S_0=0, S_1=1, S_2=2, \dots, S_{127}=127$. The K-array consists of the key, repeating as necessary times, in order to fill the array. The RC4 stream cipher works in two phases. The key setup phase and pseudorandom key stream generator phase. Both phases must be performed for every new key.

RC4 uses two counters, i and j, which are initialized to zero. In the key setup phase the S-box is being modified according to pseudo-code:

Once the Key Setup is completed the second phase encrypts or decrypts a message. The pseudorandom number generator (PRGN) phase is described by the following pseudo code:

```

Key stream generator phase:
  i = i+1;
  j = j+S (i)
  Swap S (i) and S (j)
  t = (S (i) +S (j))
  K = S (t)
    
```

Fig 3(b). Key stream generator phase

The key stream K is XORed with the plaintext / cipher text to produce cipher text / plaintext. Recent improvements make FPGAs increasingly suitable for cryptanalysis due to high density and high on chip memory bandwidth. Also it is reconfigurable for modifications in algorithms

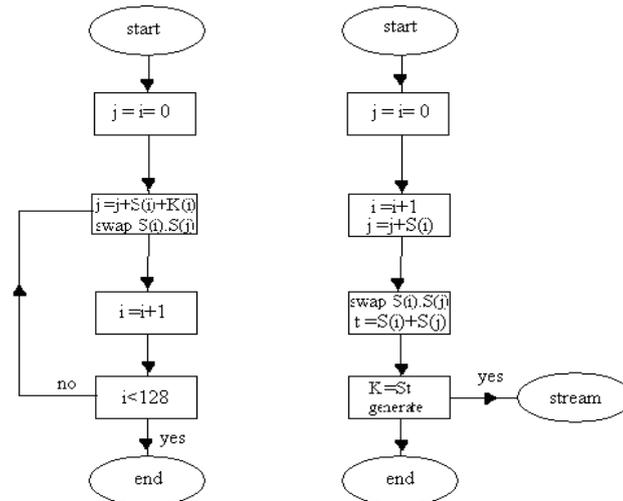


Fig 4. Algorithm of RC4 Phases

III.HARDWARE MODULE

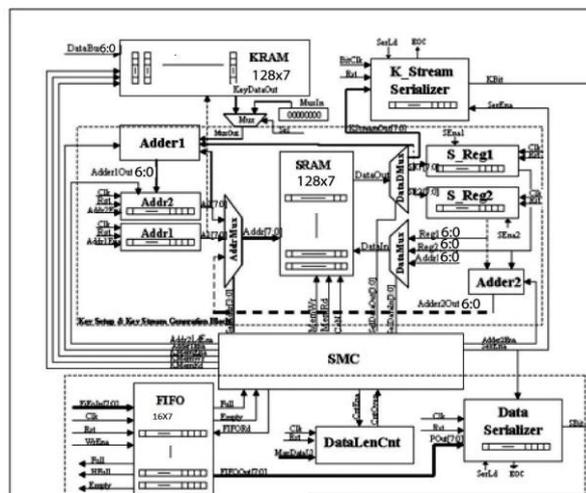


Fig.5 Hardware Module

The proposed architecture was captured by using VHDL. All the system components were described with structural architecture. The system tested using confirmed test vectors in order to examine its correctness and simulated by Modelsim simulator, Figure 5 shows out put waveforms for the same.

IV. RESULTS

Place and Route Report:

Device used xc3s400, package PQ208, speed -4.
 Device utilization summary:

Number of TBUFs	2 out of 3200 1%
Number of BUFGMUXs	2 out of 8 25%
Number of External IOBs	36 out of 141 25%
Number of LOCed IOBs	0 out of 36 0%
Number of Slices	468 out of 3584 13%

Map Report:

Target Device : xc3s400
 Target Package : pq208
 Target Speed : -4
 Mapper Version : spartan3
 Design Summary
 Number of errors: 0
 Logic Utilization:
 Number of Slice Flip Flops: 158 out of 7,168 2%
 Number of 4 input LUTs: 841 out of 7,168 11%
 Logic Distribution:
 Number of occupied Slices: 468 out of 3,584 13%
 Number of Slices containing only related logic:
 468 out of 468 100%
 Number of Slices containing unrelated logic:
 0 out of 468 0%
 Total Number 4 input LUTs: 844 out of 7,168 11%
 Number used as logic: 841
 Number used as a route-thru: 3
 Number of bonded IOBs: 36 out of 141 25%
 IOB Flip Flops: 8
 Number of GCLKs: 2 out of 8 25%
 Total equivalent gate count for design: 6,608
 Additional JTAG gate count for IOBs: 1,728
 Peak Memory Usage: 208 MB

V. CONCLUSIONS

The proposed system will be implemented for data secrecy which can be useful for variety of applications like defense, satellite TV decoders, business, stock market, internet banking.

The proposed system will have minimum hardware with increased encryption speed.

The system can use variable key length from 1 to 128 bytes providing the flexibility. Hence it will provide the higher security.

REFERENCES

- [1] "Enhancing Jian Xe, Xiaozhong Pan "An Improved RC4 Stream Cipher" International Conference on Computer Application and System Modeling (ICCASM 2010)
- [2] RC4 algorithm for WLAN WEP protocol" IEEE Transactions on control and decision conference , 2010 .
- [3] P.kitsos, G. Kostopoulos, N. Sklavos and O.Koufopavlou., VLSI design laboratory."IEEE Std 802.11. IEEE Standard: Hardware implementation of the RC4 stream cipher"
- [4] B. Schneier, "Applied Cryptography Protocols, Algorithms and Source Code in C", Second Edition, John Wiley and Sons, New York, 1996. pp. 171-184..
- [5] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996. pp. 482-504.
- [6] P. Hamalainen, M. Hannikainen, T. Hamalainen and J. Snarinen, "Hardware Implementation of the Improved WEP and RC4 Encryption Algorithms for Wireless Terminals", The European Signal Processing Conference (EUSIPCO'2000), September 5-8, 2000, Tampere, Finland, pp. 2289-2292.
- [7] Jesse Walker, "Overview of IEEE 802.11b Security", Intel Technology Journal Q2, 2000. pp. 1062-1067.
- [8] William Stallings, "Data and Computer Communication", Fifth edition, Prentice-Hall of India, 2001. pp. 624-658
- [9] Andrew S. Tanenbaum, "Computer Networks", Fourth edition, Pearson Education , 2005. pp. 292-302.
- [10] S. Fluhrer, I. Mantin, Shamir. "Weaknesses in the key scheduling algorithm of RC4 " In Proc. 8th Workshop on Selected Areas in Cryptography, LNCS 2259. Springer-Verlag, 2001. pp. 231-237.
- [11] Douglas A. Pucknell, Kamran Eshraghian, "Basic VLSI design", 3rd Edition, Prentice Hall of India, 2004. pp. 118-274.