High Speed RC4 Algorithm Based on True Dual Port RAM by using Verilog HDL

Thirupathi Naidu P, Ashok Kumar V, Kranthi R

Abstract- ***This paper presents high speed hardware implementation and an area efficient of the RC4 algorithm based on True Dual Port (TDP) RAM. The proposed architecture uses Block RAM (BRAM) implementation to reduce the area and to increase the speed of operation hence throughput. The proposed design uses only one 256 bytes True Dual Port RAM for key stream generation and it needs two clock cycles per one byte. It supports 1 byte to 256 bytes of variable key length and it achieves 71.39 MB/s throughput at 142.78 MHz maximum operating frequency. The True Dual Port RAM RC4 algorithm is implemented in Verilog HDL. The Proposed design is targeted on XC4VFX12-12SF363 Xilinx FPGA and met the operating frequency of 142.78 MHz.***

Keywords - True Dual Port RAM, BRAM, CPLD, FPGA, RC4 Algorithm and Stream Cipher.

I. INTRODUCTION

RC4 algorithm has proposed by Ron Rivest in the year of 1987. It provides one of the variable key size stream ciphers with byte-oriented operations. The RC4 algorithm has developed on the use of random permutations.RC4 is one of the used software based stream cipher.RC4 is used in Secure Socket Layers (SSL) to secure internet traffic as well as used in Wired Equivalent Privacy (WEP) to protect the wireless network. In RC4 stream cipher, byte wise swapping of S-box elements is required to perform the byte wise swapping and S-box elements required to be processed through three different steps viz. i) read i^{th} location data from the Substitution(S)-box. ii) Calculate for a new location j, read j^{th} location data from the S-box and move the i^{th} location data into j^{th} location iii) write j^{th} location data into i^{th} location. Every byte of ciphering key has generated after all three steps are performed. The implementation of hardware RC4 stream cipher has proposed in [1] takes eight clock cycles, a Fast Software Encryption of RC4 algorithm presented in [2] needs seven clock cycles, The RAM-based CPLD-Based RC-4 Cracking System design in [3] require four clock cycles, the hardware design of RC4 stream ciphers in [4] and [5] takes three clock cycles. The architecture used in [4] uses three blocks of 256 bytes RAM for swapping of S-box elements and the throughput is 22MB/sec.

In another criteria presented in [6], the register based S-box has developed and processing time is reduced to one clock cycle but the long critical path is caused by large DEMUX and MUX gates limits the core of operating frequency. In this paper, the proposed design has implemented in order to support the variable key length from 1 byte to 256 bytes. It consists of a 256 bytes True Dual Port RAM for final key stream generation and data controlling operations as well as 256 bytes Block RAM as S-box and Key register array to store the input key. The design requires 513(2*256+1) clock cycles for initial permutation of the S-box elements and then it needs 2*n clock cycles to produce the N byte of cipher data and the total duration of the RC4 algorithm consisting 513+2*n clock cycles.

Manuscript published on 30 December 2014.
***Correspondence Author(s)**

Thirupathi Naidu P, Student, Department of ECE from Aditya Institute of Technology & Management, Tekkali, Srikakulam, Andhra Pradesh, India.
Ashok Kumar V, Assoc. Prof., Department of ECE from Aditya Institute of Technology & Management, Tekkali, Srikakulam , Andhra Pradesh, India.
Kranthi R, Asst. Prof., Department of ECE from Aditya Institute of Technology & Management, Tekkali, Srikakulam, Andhra Pradesh, India.

II. RC4 STREAM CIPHER

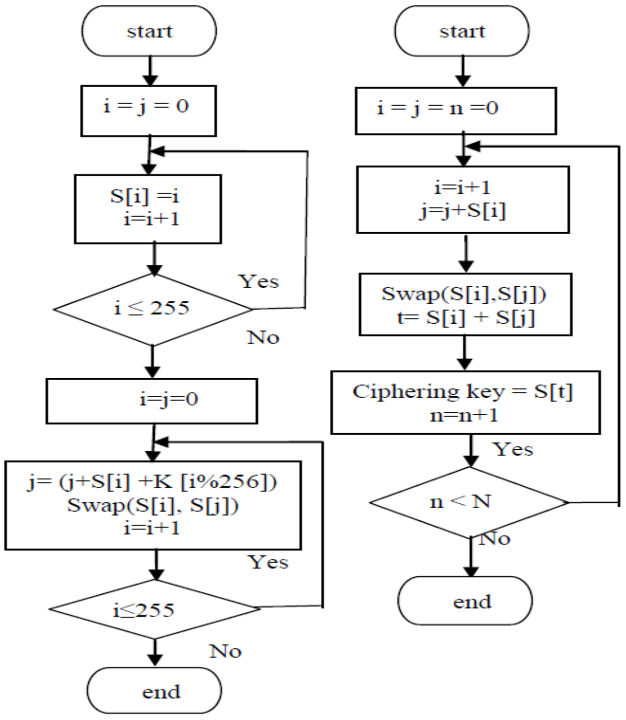

Fig. 1: RC4 Algorithm flow chart

II. a) Initialization of S-box

The values of S-box are set equal to the values from 0 through 255 in a linear manner, i.e.[0]=0,S[1]=1,S[2]=2 …,S[255]=255.

The operations can be summarized as

For i= 0 to 255

S[i] = i;

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

II. b) Initial Permutation of S

The initial permutation of the S box is explained in the following pseudo code.

```
j=0;
For i= 0 to 255
j= (j+K [i%key_len]) %256;
Swap(S[i], S[j]);
```

II. c) Key Stream Generation

Once the S vector is initialized, the input key is no longer used

Key Stream generation is explained the following code.

```
i, j = 0;
While (true)
i= (i+1) % 256;
j= (j+ S[i]) % 256;
Swap (S[i] + S[j]);
Key= {S [(S[i] + S[j]) % 256]}
```

Every generated key byte is simply XORed with incoming plaintext/ciphertext to generate cipher text/plaintext.

Data out= key XOR plaintext (Byte wise)

In fig.1, N is the number of required final key stream bytes for

encryption/decryption.

III. PROPOSED ARCHITECTURE

The block diagram of the proposed design has shown in Fig.2. It consists of controller, 256 bytes BRAM as S-box and Key register array is used to store the key. The BRAM used for the S-box is a True Dual Port RAM, it has two ports namely port A and port B. These two ports can be used in dependently for both read and write operations. The port A has the signals addra, dina, wea, douta and clka and the port B has signals addrb, dinb, web, clkb and doutb. addra, addrb signals indicates the address location of the memory to write data into that location or to read data from that location of port A, port B respectively. dina, dinb signals used to write data into specific memory location of port A, port B respectively. Data read from a memory location of port A/port B is available in the signals douta/doutb. wea, web are read, write control signals of the port A, port B respectively. In the proposed architecture The two ports of the TDP RAM, port A and port B are operates in No Change Mode and Read First Mode respectively for effective RAM utilization. In the TDP RAM based RC4 implementation the Initialization process is separated into 2 steps. In the 1st step, port A and port B fills the S-box in parallel. The port A fills the memory locations from 0 to 127, while port B fills the memory locations from 128 to 255. In the 1st step of initialization process is filled linearly, which are S [0] = 0, S [1] = 1... S [255] = 255, it needs 128 clock cycles to finish this step. In the 2nd step of initialization process, when the key_vld is asserted the key is loaded into a register array through the input key signal.

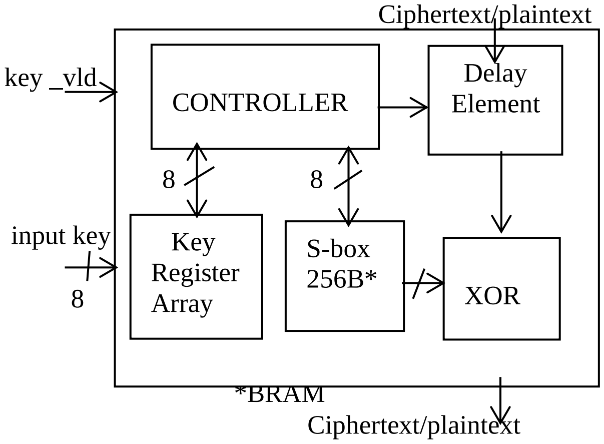

Fig. 2: Block diagram of proposed architecture

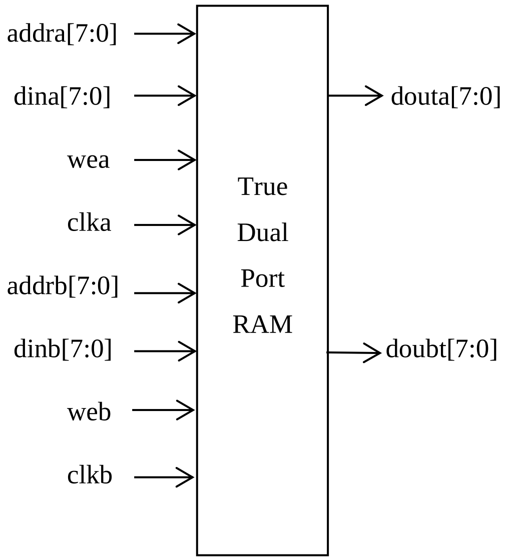

Fig. 3: Block diagram of True Dual port RAM

The initial swapping of S-box elements stored in BRAM requires two clock cycles per one iteration and the necessary control logic is implemented in the code. In the 1st clock cycle the data in the i^{th} location, S[i] is available by the read command given in the port A in the previous clock cycle, ‘j’ is calculated using S[i] and S[i] is written into the j^{th} location by using the port B, before writing the S[i] value into the j^{th} location the contents of jth location are available on the doutb signal because the is operated in Read First Mode. One is added to ‘i’ and the result asserted as read address of S[i] by using the port A, which is used in next iteration. In the second clock cycle j^{th} location data (which is available on the doutb signal by the write operation on j^{th} location in the first clock cycle) is written into the i^{th} location. This process is repeaters for 256 times to complete the initial permutation of S-box elements. It needs total 513 (2*256+1=513) clock cycles to complete the initial permutation of S-box elements. In the key stream generation phase ‘i’ and ‘j’ values calculated as per algorithm shown in Fig 5.1 and Swapping of S-box elements is performed as explained in the initial swapping. In this phase in each iteration S [{S[i] +S[j]} %256] is performed in the second cycle which gives the final key byte.

This phase is repeated as long as the input data is available. Byte wise XOR operation of final key byte with the incoming plaintext/cipher text is implemented to produce the cipher text/plaintext. Any subsequent assertion of key_vld would need all the three phases to be performed. This phase requires 2*n (n is number of bytes in the input data) clock cycles. The total duration of the RC4 algorithm consisting of 513+2*n clock cycles.

IV. RESULTS AND COMPARISON

The architecture is developed in Verilog HDL and simulated in Xilinx ISE. The whole design is targeted on Xilinx 4VFX12-12SF363 FPGA and the device implementation results are shown in Table 1.

Table1: Implementation Results

Target device: Xilinx 4VFX12-12SF363		
	Used	**Available**
Number of Slice Flip Flops	96	10,944
Number of 4 input LUTs	257	10,944
Number of bonded IOBs	27	240
Frequency	142.78MHz	
Throughput	71.39MB/s	

Table 2: Hardware Resources and Frequency Comparison

	[1]	[4]	[8]	Proposed
FPGA Device	XC400E-4013E PQ208-2	XC2V250 fg256		XC4VFX 12-12SF363
Number of Slice Flip Flops	255	138	135	96
Frequency (MHz)	40	64	164.6	142.78
Throughput (MB/s)	5	22	54.8	71.39

The results in terms of area and frequency of proposed implementation are compared with [1], [4] and [8] in Table 2.The results show the improved area and frequency of operation as compared to [1], [4] and [8]. The results show that the proposed system provides higher throughput 71.39 MB/s at 142.78MHz. It requires only 96 flops. The proposed system uses only one block of 256bytes True Dual Port RAM for S-box where as [4] uses three blocks of 256 bytes RAM for S-box.

V.CONCLUSION

In the paper a Block RAM based hardware RC4 Stream Cipher has been implemented.The area reduction and the higher operating frequencies are achieved by implementing True Dual Port RAM (BRAM) used as S-box. The processing time to produce one byte of cipher text is 2 clock cycles. The system supports a variable key length of 1 to 256 Bytes. The system provides 71.39MB/s throughput at 142.78MHz clock frequency. The work may be extended to improve the processing speed and the throughput by implementing different RAM models.

REFERENCES

1. P.Hamalainen , M.Hannikainen,T.Hamalainen and J.Saarinen, “Hardware Implementation of the Improved WEP and RC4 Encryption Algorithm for Wireless Terminals”, the European Signal Processing Conference (EUSIPCO’2000), pp.2289-2292, September 5-8, 2000.
2. B.Schneier, D.Whiting, “Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium processor” Fast Software Encryption workshop (FSE97), LNCS, Vol, 1267, pp.242-259, Springer-Verlag, Haifa, Israel, January 20-22, 1997.
3. P.D. Kundarewich, S.J.E Wilton, A.J.Hu. “A CPLD-Based RC-4 Cracking System”, the 1999 Canadian Conference on Electrical and Computer Engineering, May 1999, Vol.1, pp.397-402.
4. P.Kitsos, G.Kostopoulos, N. Sklavos and O.Koufopavlou, “Hardware Implementation of the RC4 Stream Cipher”, IEEE 46th Midwest Symposium on Circuits & Systems, Vol.3, pp.1363-1366, 2003.
5. K.H Tsoi, K H Lee and P.H.W Leong, “A Massively Parallel RC4 Key Search Engine”, Proc. Of the 10th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM02), September 22-24, 2002 Napa, California, pp.13-21.
6. S.S.Gupta, K Sinha, S.Maitra and. B.P.Sinha, “One Byte per Clock: A Novel RC4 Hardware”, 11th International Conference on cryptography-Indo crypt 2010 Dec. 2010, India.
7. William Stallings, “Cryptography and Network Security- Principles and Practice”, Fifth Edition, Prentice Hall, 2011.
8. R.Chandra Mouli, K.R.K Sastry, “Hardware Implementation of High Speed RC4 Algorithm in FPGA”, the International Journal of Computer Applications, December-2013, volume 4, 0975-8887.

AUTHOR PROFILE

Thirupathi Naidu P, pursuing M.Tech, Department of ECE from Aditya Institute of Technology & Management, Tekkali, Srikakulam and India. Research interests include the Areas of development of algorithms of Signal and Image Processing, Wireless Communication and Cryptography.

Ashok Kumar V, Assoc. Professor, Department of ECE from Aditya Institute of Technology & Management, Tekkali, Srikakulam and India. Pursuing Ph. D at GIT, GITAM University. Research interests include the areas of development of algorithms of Signal and Image Processing, Wireless Communication and Cryptography.

Kranthi R, Asst. Professor, Department of ECE from Aditya Institute of Technology & Management, Tekkali, Srikakulam and India. Research interests include the areas of Image Processing, Microwaves and Antennas.