VHDL MODELING OF THE SRAM MODULE AND STATE MACHINE CONTROLLER OF RC4

Poonam Minj[1], Shriya Sharma[2], Dinesh Kumar[3]

[1,2]Student, [3]Faculty, Department of Electronics and Telecom,

Kirodimal Institute of Technology, (India)

ABSTRACT

In this paper, VHDL modeling of the SRAM module and State Machine Controller (SMC) module of RC4 stream cipher algorithm for Wi-Fi encryption is proposed In cryptography RC4 is the most widely used software stream cipher and is used in popular protocols .The design of RC4 avoids the use of LFSRs, and is ideal for software implementation, as it requires only byte manipulations. The RC4 algorithm will implement by FPGA using VHDL software Platform STATE MACHINE CONTROLLER (SMC).

Key Words: FSM, RC4 Stream Cipher, SRAM Module, State Machine Controller, VHDL Simulation

I. INTRODUCTION TO RC4 STREAM CIPHER

Cryptographic algorithms that can provide fast implementation, small size, low complexity, and high security for resource-constrained devices such as wireless sensor devices are imperative. Conventional cryptographic algorithms are very complex and consume significant amount of energy when used by resource constrained devices for the provision of secure communication, and public key algorithms are still not feasible in sensor networks for several reasons including limited storage and excessive energy usage [1]. Therefore, security schemes should rely on a symmetric key.

II. SIMULATION OF SRAM (256× 8) MODULE

In "fig.1" Shows Pin diagram of SRAM, the module SRAM is similar to KRAM. It is used to store the data from 0 to 255 at the address from 0 to 255 i.e. same data is assigned to the same memory location.

The address is assigned by the output of Addr1.In this if Memory Write is 1 and Memory Rd is 0, then data is written in to the RAM and if Memory Write is 0 and Memory Rd is 1, then data is read out one by one from the RAM. Data is given in parallel form and is read out in parallel [6] .

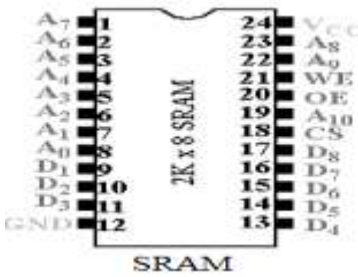

Figure1. Pin Diagram of SRAM

III. ANALYSIS OF RC4 ALGORITHM STATE MACHINE DIAGRAM

Different states of state machine Algorithm state machine diagram.

3.1Idle State

Data is at original state.

3.2 Initial State

In this state, first we fill the SRAM and KRAM. To fill both the RAM, the data is given directly to the KRAM for filling the data randomly as a Data Bus.

IV. STATE MACHINE CONTROLLER (SMC) MODULE

This is considered as the Controller (SMC) module. By this,"fig.2" shows below it can control all the modules .This state machine will work whenever Initial Over and Key Set up over are high step. First it controls Address, SRAM and KRAM. When enable is high means that it was writing key data in it. Then it is going to the input and it is given to the SRAM and this process run up to 256 times key data bytes is performed. Then it goes to Adder 2Generation.In this state, it takes the data from S _Register and gives it to the Adder that is in Adder 2Ld.It adds the given the help of Address Multiplexer, which swap it and then gives it to the K_ Steam Sterilizer. At the same time, with the help of FIFO, the available parallel data input to serial output [5].

This means that all the modules will work step by another state i.e. Adder 2Ld. In this state, adder will add the given in this process, swapping of input and then gives it to the SRAM with Key Data is given to the Data Sterilizer. Both sterilizers convert out EX-OR to give the encrypted data serially

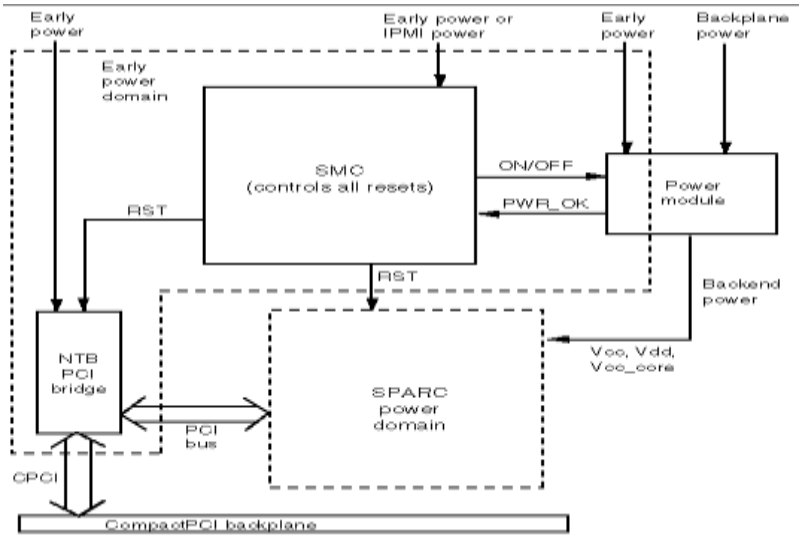

Figure2. State Machine Controller

V. PRESET LOGIC AS FSM

The preset logic in "fig.3" shows hierarchical FSM whose principal function is to generate the correct beginning addresses for all subsequent iterations .This block contains a 4-bit counter keeping track of end of states during the iteration. The FSM enters into the first state (SF) with CLR = 1. Based on the value in MOD_TYPE it makes transition to one of the four possible next states (SMT0, SMT1, SMT2 or SMT3).

Each state in this level represents one of the possible modulation schemes. The FSM thereafter makes transition to the next level of states (e.g. S000, S001 and so on) based on the value in the accumulator [4].

When the FSM at this level reaches to the terminal value of that iteration (e.g.45 in SMT0), it makes transition to a state (e.g. S000) in which it loads the accumulator with the initial value (e.g. preset=1) of the next iteration. This process continues till all the inter leaver addresses are generated for the selected MOD_TYP. If no changes take place in the values of MOD_TYP, the FSM will follow the same route of transition and the same set of inter leaver addresses will be continually be generated.

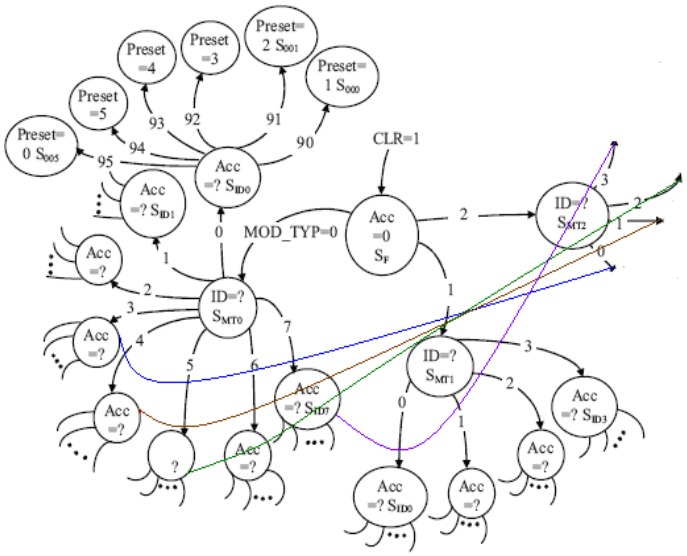

Figure3. Preset logic as FSM

VL. INTER LEAVER MEMORY FOR WLAN

The inter leaver memory block comprises of two memory modules (RAM-1 and RAM-2), three MUX .In block interleaving when one memory block is being written the other one is read and vice-versa. Each memory module receives either write address or read address with the help of the MUX connected to their address inputs (A) and set line. RAM-1 at the beginning receives the read address and RAM-2 gets the write address with write enable (WE) signal of RAM-2 active [3].

VII. SRAM CELL

A SRAM cell must be designed in such a way, so that it provides a non destructive read operation and a reliable write operation. In the conventional 6T SRAM cell this condition is fulfilled by appropriately sizing all the transistors in the SRAM cell. Sizing is done according to the cell ratio (CR). Traditional SRAM cells are symmetrically composed of transistors with identical leakage and threshold characteristics [2].

The two lines between the inverters are connected to two separate bit-lines via two n-channel pass-transistors (left and right of the cell). The gates of Those transistors are driven by a word-line. The 6T SRAM cell has a differential read operation. This means that both the stored value and its inverse are used in evaluation to determine the stored value.

VIII. CONCLUSION

Various individual modules of RC4 stream cipher for Wi-Fi security have been designed, verified functionally using VHDL Simulator, synthesized by the synthesis tool and a final net list has been created. The An innovative 6T SRAM cell concept has been proposed and validated in 45nm MCFET technology.

The simulation results have shown great potential of the proposed approach for optimizing both the cell stability and the power consumption (higher than 25%) without any area penalty and for the same read access time .well adapted for all applications ,low power and high performance.

REFERENCES

[1] Sharma K Ghose MK Kumar D, Singh RPK, Pandey VK, "A comparative study of various Security approaches used in wireless sensor networks" Int J Adv Sci Technol, 177(77), 2010.

[2] Gupta SS, Chattopadhyay A, Sinha K, Maitra S, Sinha B, " High-performance hardware Implementation for RC4 stream cipher" IEEE Trans Comput 62(4):730–743,2013.

[3]. Ahmad S, Beg MR, Abbas Q, Ahmad J, Atif S, " Comparative study between stream cipher And block cipher using RC4 and Hill Cipher" Int J Comput Appl (0975–8887), 1(25),2010.

[4]. Disha Handa, Bhanu Kapoor " State of the Art Realistic Cryptographic Approaches for RC4 Symmetric Stream Cipher", International Journal on Computational Sciences & Applications (IJCSA) Vol.No.4, August 2014.

[5]. A.M.Bhavikatti, S. Srinivas Rao "VHDL Modeling of the payload data processor and controller of RC4 stream Cipher for Wi-Fi encryption" ,ICVED-2008, Proceedings of International Conference on Embedded system & VLSI Design, 20-21 March 2008, at PDVVP College of Engineering, Ahmdnagar.

[6]. Dr.A.M.Bhavikatti, "VHDL Simulation of KRAM, Multiplexer and K Stream serializer Modules of RC4 Stream Cipher for Wi-Fi Security" ,International Journal of Advances in Wireless and Mobile Communications (AWMC) ,ISSN 0973-6972, Volume 6, Number 1, pp17-23,2013.