International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-3 Issue-3, August 2013

Hardware Implementation of ZUC Stream Cipher

Praneet .R. Shah, Naganath.B.Hulle

Abstract- Stream ciphers are more efficient as compared to block ciphers, when implemented in hardware environment, like Field Programmable Gate Array (FPGA). In this paper a high throughput hardware implementation of ZUC stream cipher is presented. ZUC is a stream cipher that forms the heart of the 3GPP confidentiality algorithm 128-EEA3 and the 3GPP integrity algorithm 128-EIA3. This algorithm offers reliable security services in Long Term Evolution networks (LTE), which is a candidate standard for the 4G network. A detailed hardware implementation is presented in order to reach satisfactory performance results in LTE systems. The design is being coded using VHDL language and for the hardware implementation, a XILINX Virtex-5 FPGA is used [1][2].

Index Terms- 3GPP, FPGA, Long Term Evolution networks security, ZUC.

I. INTRODUCTION

Nowadays there are many stream cipher algorithms proposed in both academic and industrial research.In the field of telecommunications, the world is stepping into 4th Generation (4G for short) standard. During the last few years, the 3rd Generation Partnership Project (3GPP) has submitted Long Term Evaluation Advanced (LTE-Advanced), which is the enhancement of the LTE standard, as a candidate for the 4G network [2].Long Term Evolution (LTE), is the next-generation network beyond 3G that enable fixed to mobile migrations of Internet applications such as Voice over IP (VoIP), video streaming, music downloading, mobile TV and many others. LTE networks will also provide the capacity to support an explosion in demand for connectivity from a new generation of consumer devices tailored to those new mobile applications. The current radio interface protection algorithms for LTE, 128-EEA1 for confidentiality and 128-EIA1 for integrity have been designed by SAGE/ETSI Security Algorithms Group of Experts. 128-EEA1 and 128-EIA1 are based on SNOW3G stream cipher. Also, the 3rd Generation Partnership Project (3GPP), together with the GSM Association specifies a second set of algorithms,128-EEA2 and 128-EIA2, which are based on AES block cipher. Finally, 3GPP with GSM association specifies a third set of algorithms for confidentiality and integrity the 128-EEA3 and 128-EIA3 respectively. Both ciphers are based on ZUC stream cipher. The most serious reason for these new ciphers is that LTE will be used in many countries worldwide. But Chinese regulation will not allow those algorithms to be used in China, because they were not designed in China. However, ZUC has been designed in China, and thus that it can be used in China. In this project an efficient FPGA implementation of ZUC stream cipher is presented.

Manuscript received August, 2013.

Mr.Praneet R Shah, ME (VLSI & Embedded System), G.H.R.I.E.T Wagholi, Pune, India.

Prof.N.B.Hulle, ME E&T'C, G.H.R.I.E.T Wagholi, Pune, India.

The advantages of Virtex-5FPGA are explained using the embedded functions such as Digital Signal Processing (DSP) blocks, with the aim to minimize the registers and Look-Up Tables in the design [1][3].

II. ZUC STREAM CIPHER

Cipher systems are usually subdivided into block ciphers and stream ciphers. Block ciphers tend to simultaneously encrypt groups of characters, whereas stream ciphers operate on individual characters of a plain text message one at a time. ZUC is a word-oriented stream cipher that takes a 128-bit Key and a 128-bit Initial Vector (IV) as input, and outputs a keystream of 32-bit words. ZUC has three logical layers. The top layer is a Linear Feedback Shift Register (LFSR) of 16 stages, the middle layer is for bit reorganization (BR), and the bottom layer is a nonlinear function F [2].

The LFSR has 16 of 31-bit cells ($s_0, s_1, \ldots, s_{15}$). This LFSR has two stages of operations: the initialization stage and the working stage.

In the initialization, the LFSR receives a 31-bit input word u, which is obtained by removing the rightmost bit from the 32-bit output W of the nonlinear function F, (u=W>>1). More specifically, the initialization mode works as follows:

LFSR With Initialisation Mode (u)

{1. $v=2^{15}s_{15}+2^{17}s_{13}+2^{21}s_{10}+2^{20}s_4+(1+2^8)s_0 \bmod (2^{31}-1)$;

2. $s_{16}=(v+u) \bmod (2^{31}-1)$;

3. If $s_{16}=0$, then set $\rightarrow$ $s_{16}=2^{31}-1$;

4. $(s_1, s_2, \ldots, s_{15}, s_{16})$ $(s_0, s_1, \ldots, s_{14}, s_{15})$ }

In the working mode, the LFSR does not receive any input, and works as follows:

LFSR With Work Mode

{1. $s_{16}=2^{15}s_{15}+2^{17}s_{13}+2^{21}s_{10}+2^{20}s_4+(1+2^8)s_0 \bmod (2^{31}-1)$;

2. If $s_{16}=0$, then set $s_{16}=2^{31}-1$;

3. $(s_1, s_2, \ldots, s_{15}, s_{16})\_(s_0, s_1, \ldots, s_{14}, s_{15})$ }

The bit-reorganization layer extracts 128-bit from the cells of the LFSR and forms 4 of 32-bit words, where the first three will be used by the nonlinear function F in the bottom layer, and the last word will be involved in producing the keystream. Let $s_0, s_2, s_5, s_7, s_9, s_{11}, s_{14}, s_{15}$ be eight cells of LFSR. Then the bit-reorganization forms four 32-bit words X_0, X_1, X_2, X_3 from the above cells as follows: $X_0=s_{15H} \| s_{14L}$, $X_1=s_{11L} \| s_{9H}$, $X_2=s_{7L} \| s_{5H}$ and $X_3=s_{2L} \| s_{0H}$ with respect at the rule that s_{iH} means the bits 30...15 and s_{iL} means the bits 15…0 of s_i respectively. The nonlinear function F has two 32-bit memory cells R1 and R2. Let the inputs to F be X_0, X_1 and X_2, which come from the outputs of the bit-reorganization. Then function F outputs a 32-bit word W. The detailed process of F is as follows:

F (X_0, X_1, X_2)

{ 1. $W = (X_0 \oplus R_1) + R_2$;

2. $W_1 = R_1 + X_1$;

3. $W_2 = R_2 \oplus X_2$;

4. $R_1 = S(L_1(W_{1L} \| W_{2H}))$;

5. $R_2 = S(L_2(W_{2L} \| W_{1H}))$; }

Where S is a 32 X 32 S-box and L_1, L_2 are linear transformations.

The 32X32 S-box S is composed of four 8X8 mini Sboxes, i.e., S=(S_0, S_1, S_2, S_3), where S_0=S_2, S_1=S_3. The definitions of S_0 and S_1 can be found in the official cipher specifications. L1 and L2 are linear transformations from 32-bit words to 32-bit words.

For the cipher operation firstly the key loading procedure expands the initial key and the initial vector into 16 of 31-bit integers as the initial state of the LFSR and then two stages are executed; initialization stage and working stage. In the first stage, a Key/IV initialization is performed and the cipher is clocked without producing output. The second stage is a working stage in which every clock cycle produces a 32-bit word of output [1][4].

III. PROPOSED ARCHITECTURE

The aim of the work is to ascertain that the ZUC stream cipher can operate on a recent hardware device for efficient use on LTE networks. Adder is very basic need while designing any algorithm. In previous implementation experts used Ripple Carry Adders but speed of Ripple Carry Adder is less as compared to CLA, So here I am using CLA to improve the throughput of the system.

The proposed hardware implementation of the ZUC stream cipher is illustrated in Fig. 1. The proposed system has as main I/O interfaces a 32-bit plaintext/ciphertext input and a 32-bit ciphertext/plaintext output. As a set of control logic change, the configuration of the proposed hardware system supports all stages of operation. In addition it has two inputs, a 128-bit secret key, Key, and 128-bit initialization value, IV. Our system supports, the initialization stage, the working stage and the keystream producing stage. The main parts of the proposed architecture of ZUC are the Key Loading, the Linear Feedback Shift Register (LFSR), the BR (bit-reorganization) and the nonlinear function F. Finally, a Control Unit (that is not shown in the figure) is responsible for the correct operation of the stream cipher.

The Key Loading part use a 240-bit D constant, D = d0 ||d1 ||…||d15 (where $0 \le di \le 15$ are predefined) and together with Key and IV, produce 16 substrings of 31-bit according to the following rule si = ki || di || iv_i ($0 \le i \le 15$).

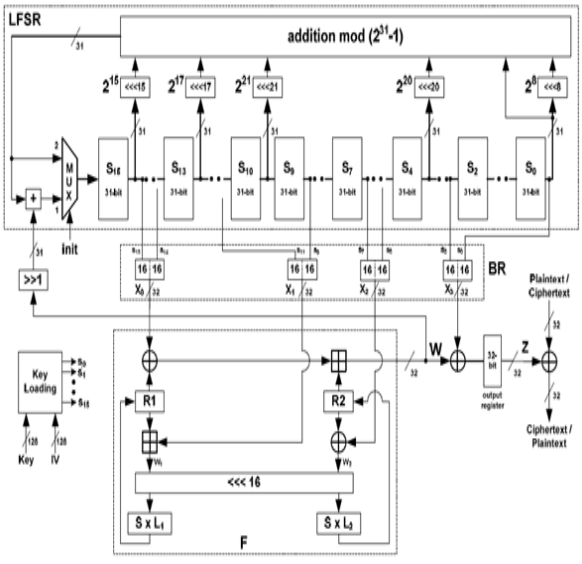

Fig.1. Proposed Architecture of the ZUC Stream Cipher

The ki and iv_i are considered the 16 bytes of the Key and IV respectively where k0 and iv0 are the most significant ones. Those substrings are used as initial values of the 31-bit LFSR cells s0, s1, …, s15 respectively. The substrings si are parallel loaded as the LFSR initial values through the OR gates as in Fig. 2. When the values are fetched the OR-gates are forced by zeros.

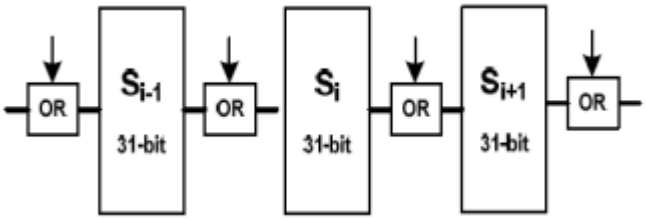

Fig.2.The 31 bit OR gates between LFSR cells

The BR consists of four simple components that execute concatenations according to the rule described previously. Only wirings are used in hardware.

The function F has two 32-bit registers R1 and R2, two S-boxes, two 32-bit XOR, two32-bit mod 2^{32} adders, two linear transformations L1 and L2 and finally a left cyclical shifter of 16 positions. The transformation L1 performs the operation.

$L_1(X) = X \oplus (X <<<_{32} 2) \oplus (X <<<_{32} 10) \oplus (X <<<_{32} 18) \oplus (X <<<_{32} 24)$ while the L2 performs the operation

$L_2(X) = X \oplus (X <<<_{32} 8) \oplus (X <<<_{32} 14) \oplus (X <<<_{32} 22) \oplus (X <<<_{32} 30)$.So each transformation uses four 32-bit XOR-gates and four left cyclical shifters.

The Feedback Logic is an arithmetic logic that combines cyclical shifters and additions mod (2^{31}-1). The multiplexer (MUX) changes their configuration according the cipher operation scenario (initialization or working stage). Also, one more adder mod (2^{31}-1) is needed with its result used as first input of the multiplexer. In the Feedback Logic six additions mod (2^{31}-1) are used. The architecture for the two inputs, X, Y, adder mod (2^{31}-1) is depicted in Fig. 3. One adder is used in order to add the values of S0 and 2^8S0, another for the addition of 2^{20}S4 and 2^{21}S10 and another for the addition of 2^{17}S13 with 2^{15}S15. Finally, a three-input adder mod (2^{31}-1) is used to add the three previous sums. For the three-input adder mod (2^{31}-1) two cascaded two-input address mod (2^{31}-1) are used.

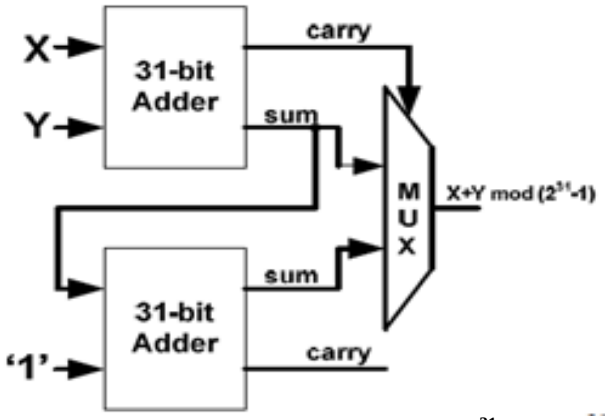

Fig.3.The architecture of Adder mod (2^{31}- 1)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The circuit that executes the Feedback Logic is illustrated in Fig. 4.

$$(S_0 + 2^8 s_0 + 2^{20} s_4 + 2^{21} s_{10} + 2^{17} s_{13} + 2^{15} s_{15}) \bmod (2^{31} - 1)$$

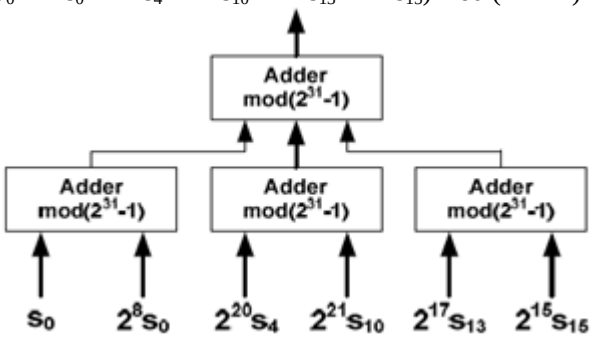

Fig.4. The feedback logic circuit

The operation of the proposed ZUC design (see Fig. 1) starts with the initial parallel loading of the LFSR initial values. Also, the values of R1 and R2 registers are set equal to zero. Then, during the initialization stage, the LFSR receives a 31-bit word as input through the multiplexer MUX (input 1 of the multiplexer is selected). This input is produced by the addition mod (231-1) between the 31-bit output of the function F called W (the rightmost bit of the output W is removed, W>>1) and the output of the feedback logic. During this operation the cipher is clocked without producing output. For this reason a 32-bit output register is located at the output of the cipher that holds the produced data. In addition, during the working mode, the LFSR does not receive any new input and input 2 of the multiplexer is selected. The cipher is executed once, and the output W is discarded. After that, the cipher produces a 32-bit keystream, Z, each clock cycle. The keystream produced by bit-by-bit XOR between the W and X3 word that is output of BR layer. In this stage of operation the 32-bit output register latches its input to the output.

IV. CONCLUSION

This proposed system uses CLA as the basic adder logic. CLA is the highest speed adder. The proposed system will be implemented for data security. As CLA in this project is implemented by NAND gates so, this reduces the cost of adder & makes the processing fast. The proposed system may increase the throughput as compared to previous implementation [1].

REFERENCES

1. Paris Kitsos, Nicolas Sklavos and Athanassios N. Skodras I, IEEE,"An FPGA Implementation of the ZUC stream cipher". 2011 14th Euromicro Conference on Digital System Design.
2. Lei Wang, Jiwu Jing, Zongbin Liu, Lingchen Zhang, and Wuqiong Pan," Evaluating Optimized Implementations of Stream Cipher ZUC Algorithm on FPGA", The First International Workshop on ZUC Algorithm Dec 2-3, 2010, Friendship Hotel, Beijing, China.
3. TANG Ming, CHENG Ping Pan, QIU ZhenLong," Differential Power Analysis on ZUC Algorithm", The 2009 International Symposium on Web Information Systems and Applications(WISA 2009) 22 – 24, May 2009 Nanchang, China.
4. Li Ji ,"Improved differential paths of ZUC", The Second International Work shop on ZUC Algorithms,June 6,2011.
5. Thomas Fuhr, Henri Gilbert, Jean-René Reinhard, and Marion Videau," Analysis of the Initial and Modified Versions of the Candidate 3GPP Integrity Algorithm 128-EIA3", The Second International Work shop on ZUC Algorithms, June 6,2011.
6. Dave Gardner," Defination of eStream Ciphers and ZUC", May 12, 2011.
7. Michalis Galanis, Paris Kitsos, Giorgos Kostopoulos, Nicolas Sklavos, and Costas Goutis," Comparison of the Hardware Implementation of Stream Ciphers", The International Arab Journal of Information Technology, Vol. 2, No. 4, October 2005,267-274.
8. Scott fluhrer ,Itsik Mantin and Adi Shamir,"Weakness in the key scheduling algorithm for RC4"Jan 2011.
9. Sandeep Kumar, Kerstin Lemke, Christof Paar," Some Thoughts about Implementation Properties of Stream Ciphers", Presentation at SASC Oct 15 2004.
10. Sourav Sen Gupta, Anupam Chattopadhyay, Member, IEEE, Koushik Sinha, Member, IEEE,Subhamoy Maitra, Bhabani P. Sinha, Fellow, IEEE," High Performance Hardware Implementation for RC4 Stream Cipher", International Journal of Cryptology Research 1(2): 225-233 (2009) ,1-15.
11. Jaya Dofe, Manish Patil," Hardware Implementation of Modified RC4 Stream Cipher Using FPGA", IOSR Journal of Engineering (IOSRJEN) ISSN: 2250-3021 Volume 2, Issue 6 (June 2012), PP 1447-1450.
12. Allam Mousa and Ahmad Hamad," Evaluation of the RC4 Algorithm for Data Encryption", Journal of ELECTRICAL ENGINEERING, VOL. 60, NO. 3, 2009, 155–160.
13. P. Kitsos, G. Kostopoulos, N. Sklavos, and 0. Koufopavlou," HARDWARE IMPLEMENTATION OF THE RC4 STREAM CIPHER", IOSR Journal of Engineering (IOSRJEN) ISSN: 2250-3021 Volume 2, Issue 6 (June 2012), PP 1447-1450.
14. N. B. Hulle , R. D. Kharadkar , A. Y. Deshmukh," Novel Hardware Implementation of Modified RC4 Stream Cipher for Wireless Network Security", International Journal of Computer Applications (0975 – 888) Volume 47– No.7, June 2012.