ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

LTE Security: EEA 3 using ZUC Algorithm

Maria Falaq, Dr. Syed Abdulhayan

M.Tech Student (Digital Electronics and Communication), Dept. of ECE, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

Professor, Dept. of ECE, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

ABSTRACT: Data security is the major concerns for wireless subscribers because their personal information is transmitted over the air and is accessible to anyone. Wireless communication systems address this problem by using state-of-the-art cryptography algorithms, such as ZUC, which has been recently integrated into the 3GPP LTE EEA-3/EIA-3 confidentiality protection methods. ZUC is a stream cipher that forms the heart of the 3GPP confidentiality algorithm 128-EEA3 and the 3GPP integrity algorithm 128-EIA3, providing reliable security services in Long Term Evolution networks (LTE), and is a candidate standard for the 4G network. An exhaustive hardware implementation is carried out in order to reach satisfactory performance goals. Stream ciphers are more efficient when implemented in hardware environment, like Field Programmable Gate Array (FPGA). The design is coded using C, which will get as a reference model, and then it is converted to Verilog HDL. Behavioral simulation (Functional Simulation) is performed first, then place, map and place & route simulations (Timing Simulations) are performed to ascertain that it works on the FPGA, XILINX Spartan3AN and Vertex-5 FPGA are used for comparison. In this work Model sim and Xilinx ISE tools are used for carrying out the work.

KEYWORDS: ZUC stream cipher, Long Term Evolution networks security, Confidentiality, FPGA, Hardware implementation.

I. INTRODUCTION

In communication systems cryptography provides integrity authentication and secrecy. The security professionals desire to achieve several goals through the use of cryptography and these goals include confidentiality, entity authentication and integrity [1]. To achieve these services all the cryptographic algorithms (ciphers) are used by communication protocols.

There are two major types of cryptographic algorithms. Symmetric algorithms make use of secret keys and the asymmetric algorithms which make use of public keys. In symmetric key cryptography, communication is protected by having both sides previously agree on the same private secret key. Usually, for exchanging of this private secret key the asymmetric cryptography is used. In asymmetric cryptography the sender makes use of a public known key in order to encrypt the message/plain text and the receiver uses their own secret key to decrypt the cipher text in order to read the message/plain text. Symmetric algorithms can be categorized into stream ciphers and block ciphers algorithms [2].

A stream cipher encrypts 1 bit or byte of plaintext at a time.The key is an infinite stream of pseudorandom bits. A block cipher encrypts a fixed size data of n-bits which is known as a block at one time. The usual sizes of each block are 64 bits, 128 bits, and 256 bits. Dedicated stream ciphers normally require less computation compared to the block ciphers for achieving the same security level. Another advantage of stream ciphers is that they do not suffer from the error propagation that occurs in block ciphers [3]. This is the due to the independent bit encryption and decryption. Also they can be implemented easily in both hardware and software compared to block ciphers and they have greater software efficiency. As a result stream ciphers have been used in several telecommunication protocols, especially wireless ones such as Long Term Evolution (LTE), Bluetooth, and Global System for Mobile (GSM).These days there are many stream cipher algorithms in both academic and industrial research.

The increasing desire for high speed data has made Long Term Evolution (LTE) one of the most favored Fourth Generation (4G) cellular networks worldwide. LTE is being deployed around the globe by cellphone operators for voice and data streaming. Earlier 3G networks made Wi-Fi a dominant technology for high-speed data when present but today LTE obtains data on cellphones even where Wi-Fi is present. LTE has improved data rates over 2G, 3G and 3.5G technologies.4G has several differences from 3G and preceding technologies. LTE systems have all flat IP based

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

architecture and lesser number of elements. The number of 4G subscribers is expected to increase dramatically and expected to reach 4.1 billion LTE subscriptions by the end of 2021[4].This gives a consensus to hackers and organizations for information theft since radio waves are exposed and available without slowing down the connection. Hence there is a trade-off between security algorithms and speed.

There are three types of cryptographic algorithms that work on LTE. Each type of cryptographic algorithm in turn is based on core algorithm which can be SNOW 3G, AES algorithm and ZUC Algorithm. 128-EEA1/128-EIA1 is based on SNOW 3G algorithm and have been designed by SAGE/ETSI Security Algorithms Group of Experts, 128-EEA2/128-EIA2 is based on AES algorithm and is specified by 3rd Generation Partnership Project (3GPP) together with the GSM Association. 3GPP with GSM association finally specifies a third set of algorithms for confidentiality and integrity, 128-EEA3/128-EIA3 which is based on ZUC algorithm

ZUCis a stream cipher designed in China. The first algorithm is 128-EEA3, which is used in the encryption process designed using ZUC and the second algorithm is 128-EIA3 which used for integrity and is designed using a universal Hash Function with ZUC as its core.

The main aim is to make the verification and evaluation of EEA3 algorithm using ZUC. This study will help to made a clear idea EEA3 using ZUC in comparison of those already in use in the UMTS network.

II. RELATED WORK

In [7] authors examined the security performance of the current LTE network as well as the vulnerabilities were also explored. Pre-existing solutions were thoroughly investigated and it was observed that there still are security issues in the current framework. The survey pointed towards the possible research issues for further investigation. In [8] authors surveyed the internal construction of the ZUC algorithm. In addition its diverse operating modes were assessed to get the idea about the space as well as time complexity in comparison to the security algorithms already in use. It was established that ZUC has a linear time complexity which assures algorithm rapidity and efficiency and at the same time having constant space complexity which is a promising result for memory constrained environments like cell phones. In [9] authors the new set of confidentiality and integrity algorithms that use ZUC as the core were evaluated and compared with those previously in use in UMTS networks. The two sets are observed to have linear time and space complexity.In [10] authors implemented ZUC stream cipher using reconfigurable execution by using Carry Look Ahead header. It was observed that the usage of the adder led to increased throughput.In [11] authors studied the effect of DPA on insecure ZUC hardware and it was observed that the algorithm happens to be vulnerable to these DPA attacks. Masking if employed in a proper way was found to be a suitable defence against DPA attacks. In [12] authors propose the usage of FCSR in place of LFSR.FCSR has a higher nonlinearity in comparison to LFSR in which Berlekamp-Massey algorithm can be used to anticipate the sequences.

III. ZUC STREAM CIPHER

ZUC is the core of standardized 3GPP confidentiality and integrity algorithm 128-EEA3 and 128-EIA.ZUC has three logical layers. The structure of ZUC stream cipher is shown in Fig 1. ZUC has two 128-bit inputs; it takes a 128 bit initial vector (IV) and 128 bit initial key and outputs a key stream of 32-bit words. Key stream is used for encryption and decryption. Execution involves two stages (1) Initialization Stage (2) Working Stage.

In the Initialization stage cipher is clocked without producing the output. In the working stage with every clock pulse a 32 bit output word is produced.

ZUC consists of three logical layers. The top layer is a linear feedback shift register (LFSR) which is of 16 stages (s0, s1, . . . , s15), each holding 31 bits. The feedback is a primitive polynomial over the finite field GF(2^{31} -1).The middle layer is for bit reorganization (BR) which extracts 128 bits from the registers of the LFSR and forms four 32 bit words. These four 32 bit words will be used by output of key stream nonlinear function F.The bottom layer is a nonlinear function F and is based upon two 32-bit memory cells $R1$ and $R2$.The nonlinear function F uses two S-boxes $S0$ and $S1$and takes 3 of 32-bit words from the BR as its inputs. It also involves different operations such as addition modulo 2^{32} the exclusive-OR and the cyclic shift [5].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

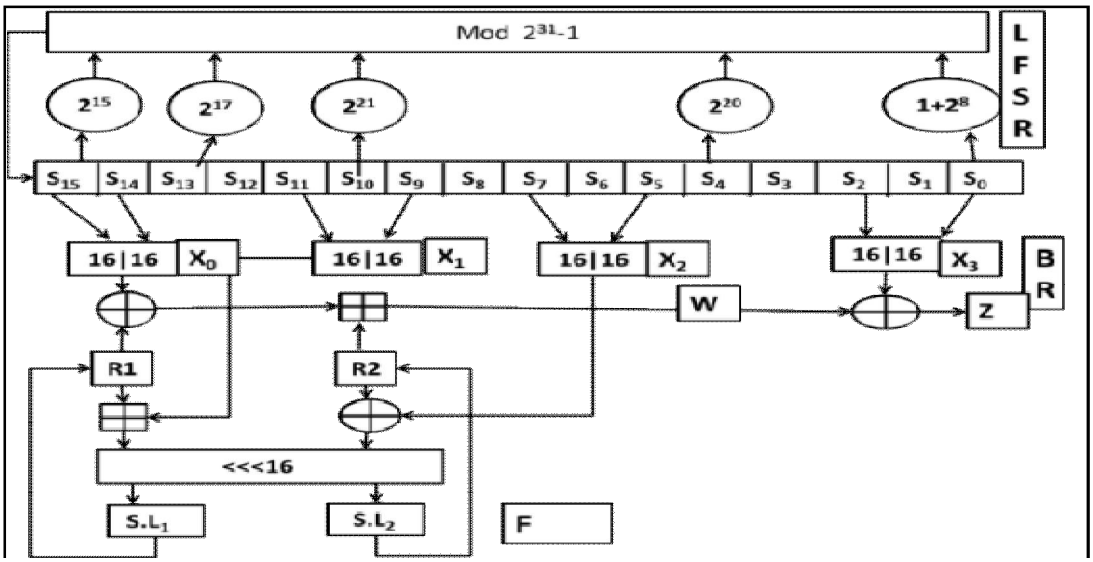

Fig. 1. ZUC Stream Cipher Architecture

A. Linear feedback shift register (LFSR).

It consists of 16 stages (s_0, s_1, . . .,s_{15}) of 31-bit registers, and each register is an integer in the set {1, 2, . . . , 2^{31}–1}.LFSR operates in two modes Initialization and Working according to the guidelines.

During the initialization stage, the LFSR receives a 31-bit input word u. It is obtained from the output nonlinear function F by removing the rightmost bit from the 32-bit output W, (u=W>>1). The LFSR stage does not receive any input during the Working mode. The initialization mode works as follows:

The initialization mode works as shown by the algorithm

Algorithm 1-

LFSR Initialization 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. $s_{16}= (u+v)\bmod(2^{31}-1)$;
3. If $s_{16}=0$, then $\longrightarrow$ set $s_{16}=2^{31}-1$;
4. $(s_0, s_1, \ldots, s_{15}) \longrightarrow (s_0, s_1, \ldots, s_{16})$ *}*

The LFSR does not receive any input in the working mode, and it works as shown by the algorithm

Algorithm 2-

LFSR 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 $\longrightarrow$ set $s_{16}=2^{31}-1$;
3. $(s_0, s_1, \ldots, s_{15}) \longrightarrow (s_0, s_1, \ldots, s_{16})$ *}*

B. The Bit-Reorganization

The middle layer of ZUC algorithm is the bit-reorganization (BR). BR extracts 128 bits from the registers of the LFSR and form four of 32-bit words. The first three of these will be used by non-linear function F in the bottom layer and last word will be used in generating key stream in F. Suppose that s_0, s_2, s_5, s7, s9, s11, s14, s15are the 8 registers of LFSR. Then the bit-reorganization generates 4 of 32-bit words namely X_0, X_1, X_2, X_3 from the above registers of LFSR as the algorithm 3.

The concatenation of signal in hardware when compared with software implementation is only needed to change the signals order and it extra time is not needed to do this work. Hence the nonlinear function operation can be mixed with bit-reorganization stage together to save clock cycle.

Algorithm 3-

1. $X_0=s_{15H}||s_{14L}$;
2. $X_1=s_{11L}||s_{9H}$;
3. $X_2=s_{7L}||s_{5H}$;

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

4. $X_3=s_{2L}||s_{0H}$;

Here s_{14L}denotes the rightmost 16 bits (15...0) of integer s_{14} and s_{15H} denotes the leftmost 16 bits (30...15) of integer s_{15}, $s_{15H}||s_{14L}$ denotes the concatenation of s_{15H} and s_{14L}.

C. The nonlinear function F

The nonlinear function F consists of two of 32-bit memory registers namely R1 and R2. The description of non-linear function Fis as follows. The input of the nonlinear function are the output of the bit reorganization step that is X_0, X_1, X_2 .The output of nonlinear function F is a 32-bit word W. In the non-linear function F, Sis the 32 x 32 S-box layer and L1 and L2 are linear transformations. The output of non-linear function Fis a 32-bit word *W*. The key stream word *Z* is given as $Z = W \oplus X3$ .The operation of non-linear function is defined by the algorithm below.

Algorithm 4-

$F(X_0, X_1, X_2)$ {

I. $W= (X_0 \oplus X_1 \boxplus) R_{21}$;

II. $W_1=R_1 \boxplus X_1$;

III. $W_2=R_2 \boxplus X_2$;

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

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

For the cryptographic operation firstly the key loading procedure will expand the initial vector and initial key 16 31-bit integers as the initial state of the LFSR. After this two stages will be executed that is the initialization stage and working stage. In the first stage an IV/Key initialization is executed and the cipher is clocked without generating the output. The second stage which is the working stage in which every clock cycle produces a 32-bit output word.

IV. CONFIDENTIALITY ALGORITHM EEA3

LTE encryption algorithm, 128-EEA3 is the described using ZUC algorithm as shown in Fig 2. The 128-EEA3 is a stream cipher and confidentiality algorithm. This cipher that is used to encrypt and decrypt blocks of data using confidentiality key CK. The maximum length of data block may be between 1 and 20000 bits.

In order ensure data confidentiality like the other cryptographic algorithms in the LTE network, the EEA3 algorithm is initialized with the confidentiality key CK and the input parameters DIRECTION, BEARER, COUNT-C. 128-EEA3 algorithm uses the ZUC stream cipher as a kernel.

There are three principal stages during the EEA3 operation initializing the key stream generator, generation of key stream and lastly data encryption/decryption.

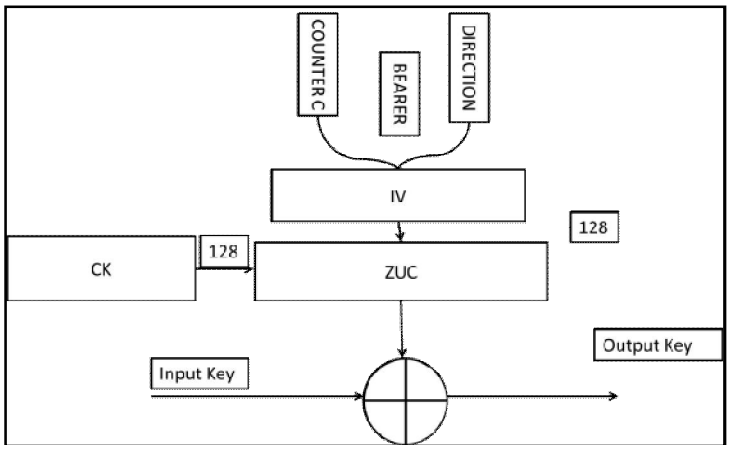

Fig. 2. Principles of the 128-EEA3 encryption operation

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

V. SIMULATION RESULTS

The Design of ZUC Stream cipher and EEA3 Algorithm if first carried out in C code as per the 3GPP standard ZUC EEA3 algorithm, The C code is then converted to Verilog HDL. The Code is simulated and verified with the C code to match the standard test cases as per the 3GPP standard. Functional and Timing simulations were performed. The design is implemented and synthesized with XILINX ISE tool FPGA used is Artix7 Family FPGA, Device XC7A0100T, Package CSG324, Speed Grade-3.The design is working at Maximum Frequency of 377.790MHz.The previous ZUC algorithm was working at 300MHz.The simulation results of Verilog matched with the C output as per the 3GPP standard.

VHDL code is verified and simulated by making use of test vectors as shown in Fig 3.In order to design the confidentiality 128-EEA3 algorithm C code is used as shown in Fig 4.

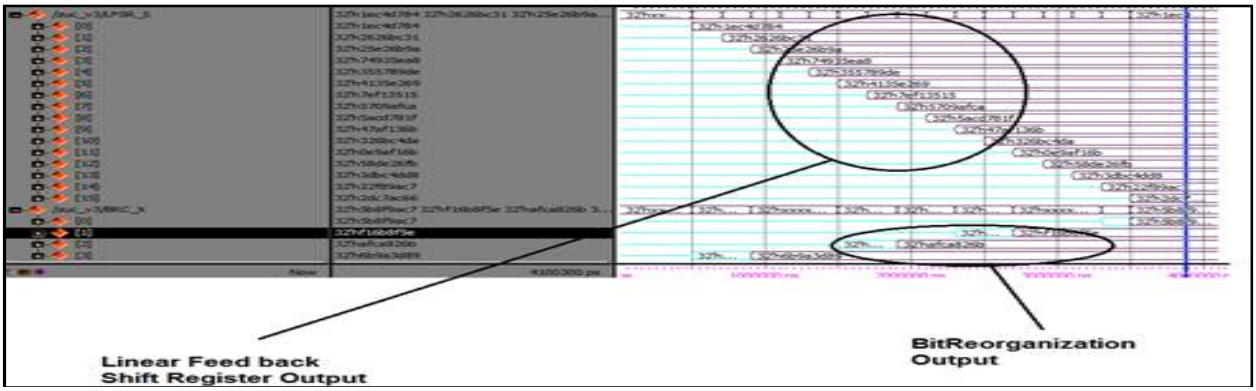

Fig. 3. Verilog Output

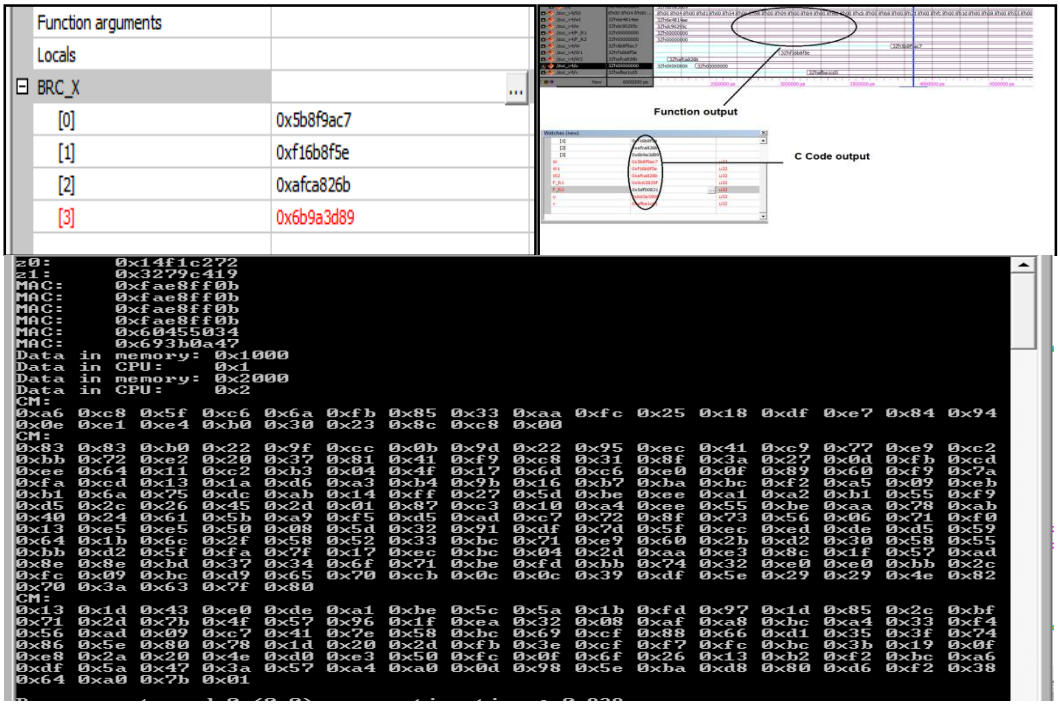

Fig. 4. C code Output

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

The RTL representation of LFSR is shown in Fig 5.Fig 6 shows the complete implementation of ZUC algorithm including the three layers-LFSR,Bit-Reorganization and the Non-linear function F. This forms the core of the EPS confidentiality algorithm 128-EEA3.

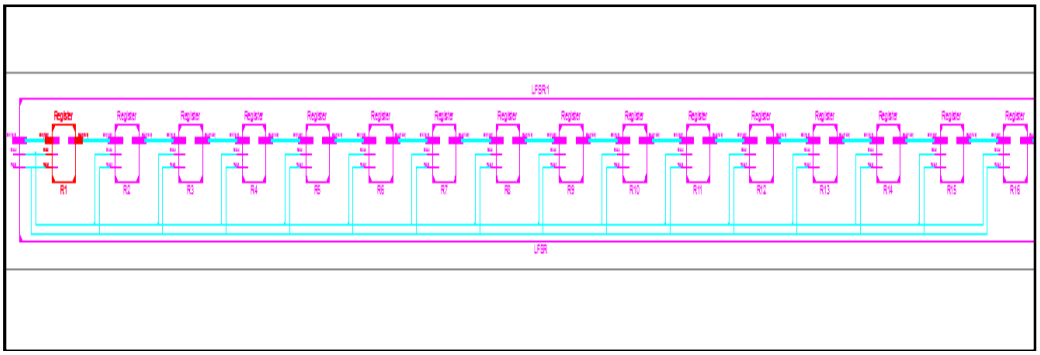

Fig. 5. RTL Schematics LFSR

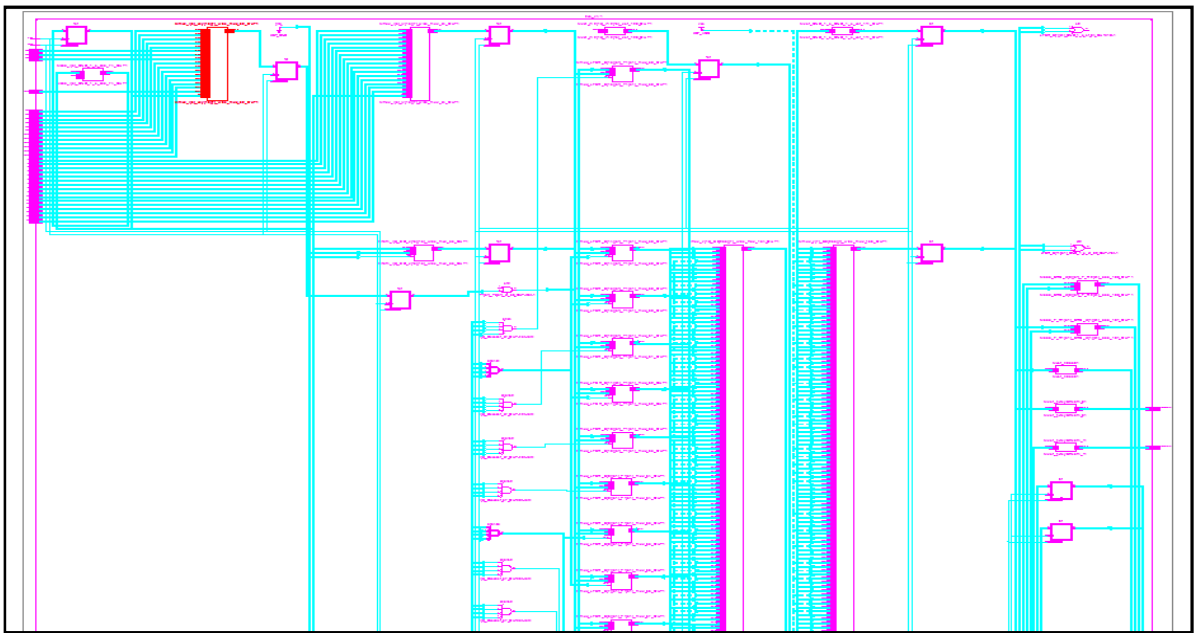

Fig. 6. Complete ZUC (with LFSR, Bit reordering, and Function)

VI. CONCLUSION

128-EEA3 is implemented and verified by C code and using Verilog as well. As specified by the 3GPP standard it was found that the simulation outcomes are similar. The design is found to be working at the speed of 377.790MHz as which leads to higher throughput and efficiency as well as faster algorithm operation as required by LTE framework. The system will be implemented for securing the data.

REFERENCES

1. Douglas R. Stinson, “Cryptography-Theory and Practice”, third ed., Chapman and Hall, CRC,pp.1-10, 2005.
2. Bruce Schneier, “Applied Cryptography – Protocols, Algorithms and Source Codein C”, second ed., John Wiley & Sons, New York, pp.1-5, 1996.
3. Jonathan Katz, Yehuda Lindell, “Introduction to Modern Cryptography: Principles and Protocols”, first ed., Chapman and Hall, CRC, pp.60-86 2007.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

4. Ericsson Mobility Report, Ericsson, November 2015.
5. ETSI/SAGE Specification, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3.Document 1:128-EEA3 and 128-EIA3 Specification; Version: 1.6, (2011).
6. ETSI/SAGE Specification, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128- EIA3. Document 2: ZUC Specification, Version: 1.6, (2011).
7. Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and ZhenxingLuo, "A Survey on Security Aspects for LTE and LTE-A Networks", IEEE communications surveys & tutorials, Vol. 16, Issue no. 1, pp.283 – 302, 2014.
8. GhizlaneOrhanou, Said El Hajji, AbdelmajidLakbabi, Youssef Bentaleb,"Analytical evaluation of the stream cipher ZUC",Proceeding of the IEEE 3rd International Conference on Multimedia Computing and Systems (ICMCS'12), pp.927 - 930, May 2012.
9. GhizlaneOrhanou and Said El-Hajji, "The new LTE cryptographic algorithms EEA3 and EIA3 verification, implementation and analytical evaluation," Applied Mathematics & Info. Sciences Journal 7, No. 6, pp.1-6, 2013.
10. Praneet R Shah, N.B.Hulle, "Reconfigurable hardware for ZUC stream cipher," IJARCSSE, Volume 4, Issue 2, February 2014.
11. Tang Ming, ChengPingPan, Qiu Zhen Long, "Differential power analysis on ZUC algorithm," Chinese Journal of Electronics, May 2012.
12. A.VijayaBhaskar, C.Ravi and Shankar Hanuman, "ZUC stream cipher using feedback carry shift register", IJEST, Vol. 4,No.06,June 2012.

BIOGRAPHY

Maria Falaq isanM.Tech Student in Digital Electronics and Communicationin the Electronics and Communication Department, DayanandaSagar College of Engineering, Bangalore, Visvesvaraya Technological University. She received B-Tech degree in 2014 from B.G.S.B University,Rajouri,J&K. Her research interests are communication, cryptography and HDL languages etc.