IRAQI Academic Scientific Journals
العــــراقيــة المجـــلات الأكـاديـمـيـة العـلـمـيـة

Al-Kut University College Journal

ISSN (E) : 2616 - 7808 II ISSN (P) : 2414 - 7419
www.kutcollegejournal.alkutcollege.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq

Vol. 9 , Issue 1 , June 2024

ZUC Ciphering Algorithm Based on Two 32-Bit Key in the Non-Linear Function for 4G Wireless Mobile Systems

Natiq Abdullah Ali [1]

Abstract

Long Term Evolution (LTE) is one of the mobile systems that used in Fourth Generation (4thG) cellular networks. The LTE stream cipher algorithm is called Zu Chongzhi (ZUC) algorithm. The ZUC is a set of rules and is the core of the Confidentiality algorithm EEA3. This paper offers with improving the security of data transmission in 4G networks. Hence, an attempt to enhance the encryption and de-encryption times is done throughout this work. In this paper, the ZUC algorithm is upgraded by adding two 32-bit keys in the non-linear function layer. Upgraded ZUC (U-ZUC) is the core of the confidentiality algorithm EEA3 which is also upgraded. The obtained results show that the proposed algorithm exhibit good encryption and de-encryption times as compared with ZUC and U-EEA3 algorithms. All the algorithms presented in this work are simulated and tested by Matlab software ver. 2022b.

Keywords: 4th G, ZUC, Long Term Evolution, encryption

Affiliation of Author
[1] Kut University College, Wasit, Iraq, 52001

[1] nataaq.abdallh@alkutollege.edu.iq

[1] Corresponding Author

Paper Info.
Published: Jun. 2024

خوارزمية تشفير ZUC تعتمد على مفتاحين 32 بت في الوظيفة غير الخطية لأنظمة الـ 4th G اللاسلكية المتنقلة

ناطق عبدالله علي [1]

الخلاصة

يعد التطور طويل المدى (LTE) أحد أنظمة الهواتف المحمولة المستخدمة في شبكات الجيل الرابع (4thG) الخلوية. تسمى خوارزمية تشفير الدفق LTE خوارزمية (Zu Chongzhi ZUC). خوارزمية ZUC هي جوهر الخوارزمية السرية EEA3. تتناول هذه الورقة تعزيز أمن نقل البيانات في شبكات الجيل الرابع. وبالتالي ، تم إجراء محاولة لتحسين أوقات التشفير وفك التشفير خلال هذا العمل. في هذا البحث ، تم تغيير خوارزمية ZUC عن طريق إضافة مفتاحين 32 بت في طبقة الوظائف غير الخطية. ZUC المحدث (U-ZUC) هو جوهر خوارزمية السرية EEA3 التي تم تغييرها أيضًا. أظهرت النتائج التي تم الحصول عليها أن الخوارزمية المقترحة تبين أوقات تشفير وإلغاء تشفير جيدة مقارنة بخوارزميات ZUC و U-EEA3. تم محاكاة جميع الخوارزميات المقدمة في هذا العمل واختبارها بواسطة برنامج .Matlab ver. 2022b

الكلمات المفتاحية : الجيل الرابع، ZUC ، تطور طويل الأمد، تشفير

انتساب الباحث
[1] كلية الكوت الجامعة، واسط، العراق،52001

[1] nataaq.abdallh@alkutollege.edu.iq

المؤلف المراسل [1]

معلومات البحث
تأريخ النشر : حزيران 2024

1. Introduction

The 4thG is one of the important communication networks for mobile system. The security related to well-known 4thG standards including WiMAX and 3GPP Long Term Evolution (LTE) has been analyzed, in this work, LTE security will be explained [1].

However, unlike in the past, LTE devices have to inform the user if encryption is used in the air interface. [2,3]. ZUC algorithm is a stream cipher algorithm and has a 128-bit initial key and a 128-bit initial vector IV as input, and outputs a keystream of 32-bit words. In this chapter will be study and analyze the ZUC algorithm. Figure (1) shows the structure of ZUC algorithm [4].

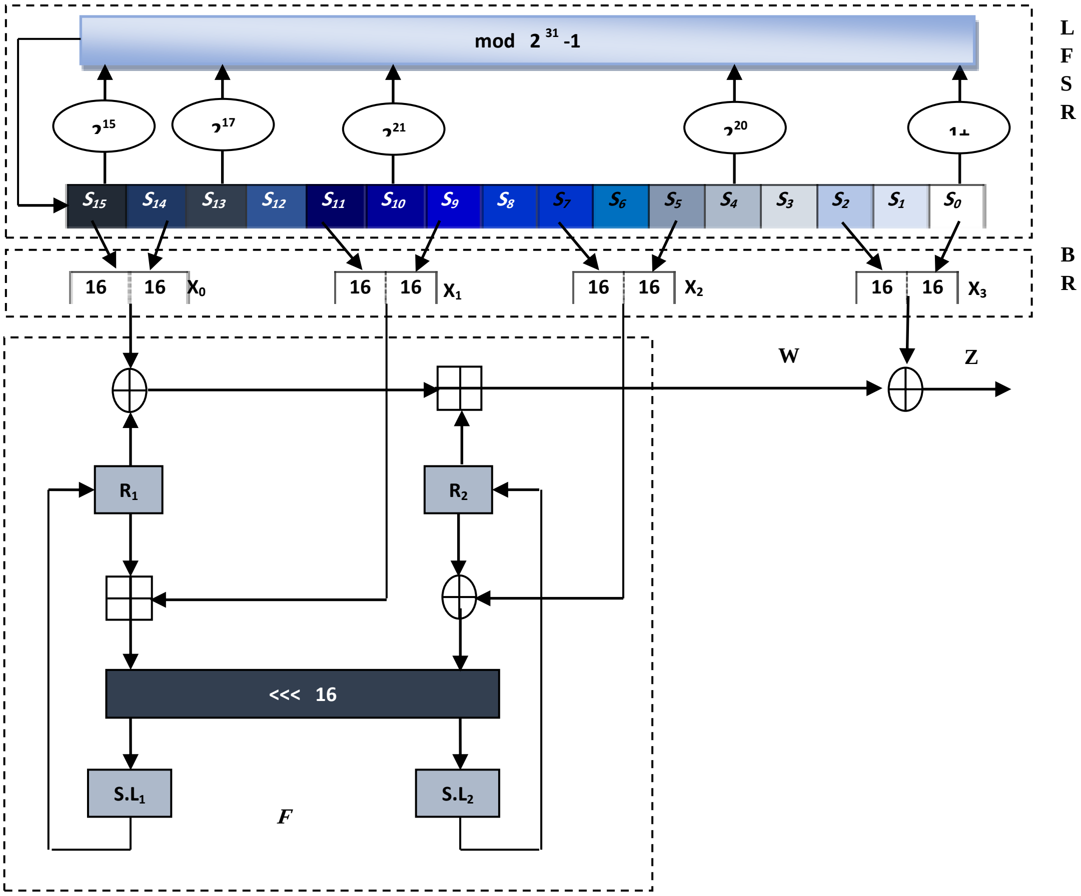

Figure (1) : The General Structure of ZUC [4]

The ZUC algorithm takes a 128-bit initial key and a 128-bit initial vector as input, and outputs is a keystream of 32-bit words, that is used for encryption/decryption the plain and encrypted data. There are two phases (stages) in the execution of the ZUC algorithm: initialization stage and working stage. In the first stage of ZUC, it performs key/IV initialization procedure, i.e., the cipher is clocked without producing output. The second stage is a working stage and the algorithm produces a 32-bit word of output per loop of the working stage with every clock pulse [5,6]. ZUC is composed of three logical layers. The top layer of the ZUC is a Linear Feedback Shift Register (LFSR) which consists of 16 stages; the middle layer is bit-reorganization (BR) procedure, and the bottom layer is a Nonlinear Function *F* procedure [4].

The aim of this paper is to proposed a modified version of ZUC ciphering algorithms to enhance the encryption time of the ZUC algorithm. Also, a confidentiality algorithm EEA3 has been proposed.

2. Literature Review

G. Orhanou , S. Elhajji , Y. Bentaleb and J. Laassiri, 2010 [2], have interested in the security features and the cryptographic algorithms that used to make ensure confidentiality and integrity of the transmitted data.

P. Kitsos, N. Sklavos, G. Provelengios and A. N. Skodras, 2013 [7], have implemented of six representative stream ciphers and compared in terms of performance, consumption area and the throughput-to-area ratio for the hardware.

Mayur Solanki, Seyed mohammad Salehi, and Amir Esmailpour, 2013 [8], have proposed an algorithm that advances efficiency within that balance for LTE one of the most popular Fourth Generation (4G) cellular networks based on AES algorithm.

Natiq Abdullah Ali and Mays A. Anaee 2015 [9], have proposed ZUC algorithm to decrease the encryption/decryption times and increase the security level of the mobile systems for the 4thG.

V. Kaula, B. Nemadeb, V. Bharadic, S. K. Narayan khedkard, 2016 [10], the authors in this work introduced designing, implementation, evaluation and also the comparison of the enhancements of security in data transmission for next generation encryption.

Zakaria Hassan Abdel Wahab, Talaat A. Elgarf & Abdelhalim Zekry, 2020 [11], the authors propose three different systems for enhancing the security levels of SNOW and ZUC algorithms.

3. The Proposed ZUC and EEA3 Algorithms

In this section, ZUC algorithm based on using two 32-bit keys in the non-linear layer will be proposed. Also, EEA3 algorithm will be proposed.

3.1 The Proposed ZUC Algorithm

In this proposed ZUC algorithm, changes in all layers of the ZUC algorithm have been made. In the first layer Linear Feedback Shift Register layer (LFSR): changes in this layer are obtained in the number of bits to be recycled to the left, which leads to change in equations (v) in the initialization mode and (S_{16}) in the work mode. Then, in the second layer Bit-Reorganization layer (BR): 32 bit-words have been chosen to form three words instead of four words (as in the original) to reduce the storage space and by using the word (X_1) as an input for the two words (W_1 *and* W_2). This will lead to change in equations (W_1 *and* W_2) that are found in the third layer Nonlinear Function layer (F) as shown in Figure (1). In Bit-Reorganization layer, the changes are to create three words (X_0, X_1 and X_2), and by taking (X_1) XORed with a key. The result of ($X_1 \oplus key$) is the input to (W_1 *and* W_2). This will lead to change in equations of this layer. This in turn leads to a change in the third layer (Nonlinear function layer) of the proposed algorithm. Also, the expression of (W_1) is also changed from mod to XOR as shown in Figure (2). The new upgraded equations of the proposed ZUC algorithm are as follow:

- In LFSR with Initialization Mode (u)

$$v = 2^{11}S_{15} + 2^{17}S_{13} + 2^{15}S_{10} + 2^{20}S_4 + (1 + 2^7)S_0 \, mod \, (2^{31} - 1)$$

- In LFSR with Work Mode ()

$$S_{16} = 2^{11}S_{15} + 2^{17}S_{13} + 2^{15}S_{10} + 2^{20}S_4 + (1 + 2^7)S_0 \, mod \, (2^{31} - 1)$$

- In Bit-Reorganization ()

$X_0 = S_{15}H \mid\mid S_{12}L$

$X_1 = S_7L \mid\mid S_{10}H$

$X_2 = S_0H \mid\mid S_5L$

- In Nonlinear Function

$F\ (X_0, X_1)$

1. $KEY1\_WITH\_X1\ = (Key1 \oplus X1)$
2. $KEY2\_WITH\_X1\ = (Key2 \oplus X1)$
3. $W_1 = R_1 \oplus (KEY1\_WITH\_X_1)$
4. $W_2 = R_2 \oplus\ (KEY2\_WITH\_X_1)$

$F\ (X_0, X_1)$

1. $W_1 = R_1 \boxplus X_1$
2. $W_2 = R_2 \oplus X_1$

Informative note : The key in the structure of ZUC algorithm is obtained from a random numbers.

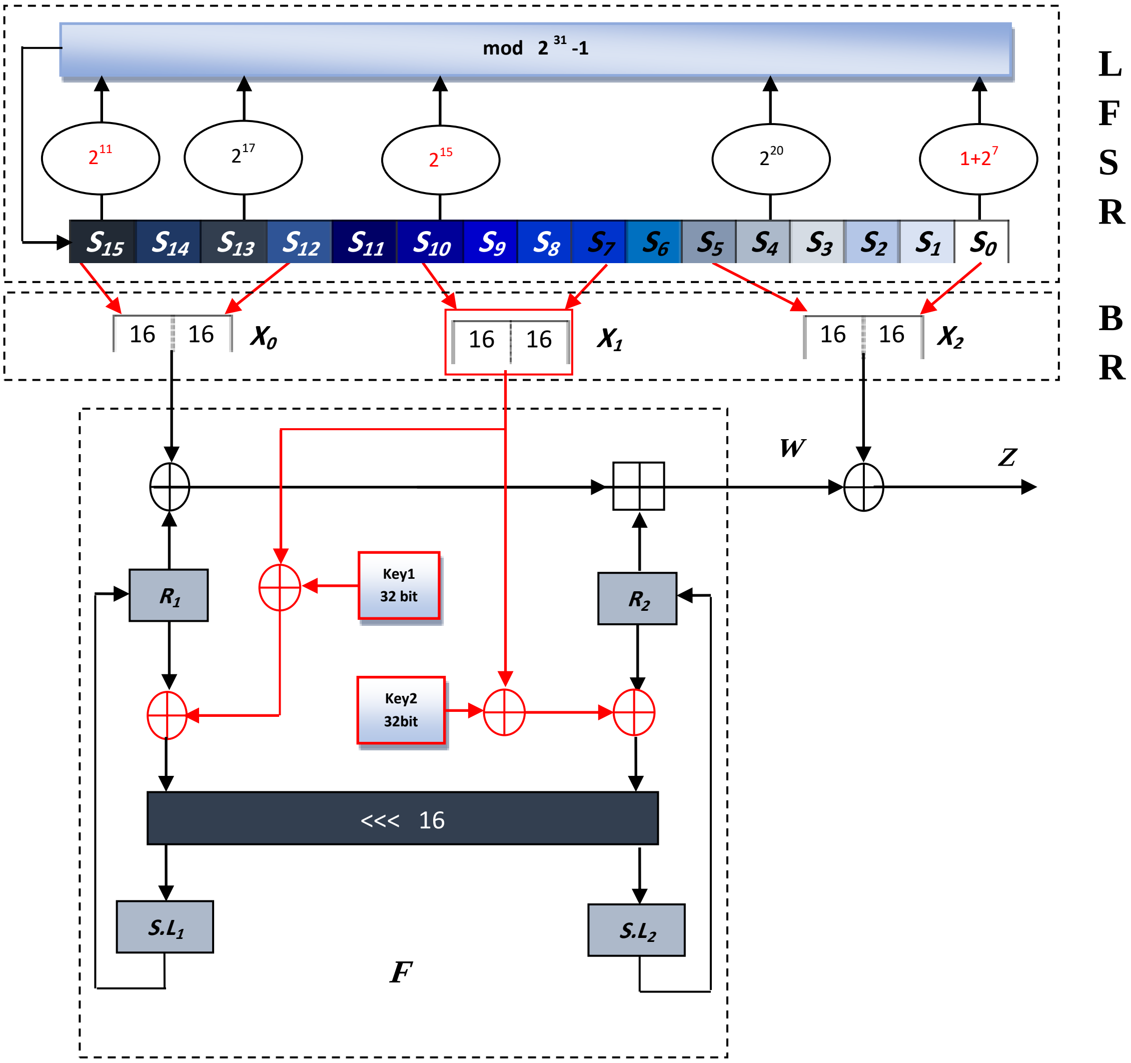

Figure (2): The Structure of the Proposed U-ZUC algorithm

3.2 The Proposed EEA3 Algorithm

In this sub-section, a modified version of confidentiality algorithm EEA3 is proposed. This is mean a modification in the EPS Encryption Algorithms EEA3. The EEA3 is a stream cipher algorithm used to encrypt/decrypt data to prevent attacks to know the data that transmit between sender and receiver. The proposed EEA3 algorithm work with internal of 128-bit blocks under the controling of a 128-bit of input key; the same as of EEA3. The U-ZUC algorithm is regard to be core of the proposed EEA3 algorithm in order to increase the security level and to reduce encryption time in the LTE 4th G mobile system. The 192 and 256 bits could also be used in this algorithm. The structure of the proposed EEA3 which we called Upgraded EEA3 (U-EEA3) algorithm is shown in Figure (3). From Figure (3) it can be shown that the U-ZUC algorithm have (IV and CK) as input parameters, each of them is a 128-bit, and also has a keystream *Z* as an output of the proposed algorithm. Keystream is added to the plaintext (IBS) by XORing operation. The result of this process is added to 128/192/256 bits key created randomly by XORing operation. Then the obtained result is the ciphertext (OBS). The keystream length is 23-bits in each loop. To find a number for the U-EEA3algorithm, the loop is then given by: length plaintext/32. Therefore, if the plaintext length has a 128-bits, the length of the algorithms' loops is 4 that produces 4-words, each word is XORed with 32-bits plaintext to get a result that will be XORed with a key in the EEA3 algorithm to obtain the ciphertext.

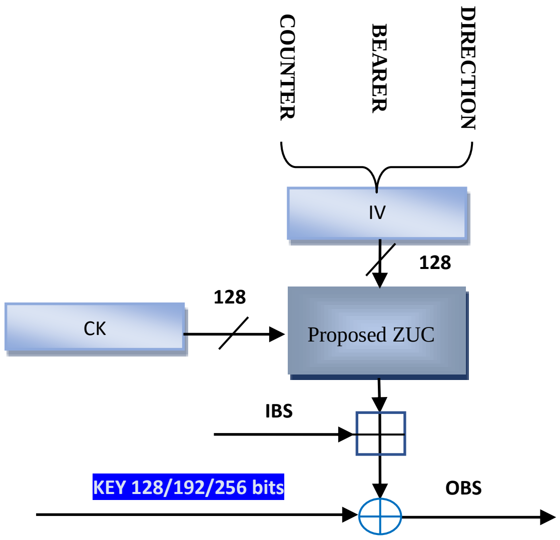

Figure (3) : The U-EEA3 Algorithm

4. Results and Discussion

The results of the proposed algorithms; U-ZUC and U-EEA3 are presented in following sub-sections, with 128 bits. Due to the randomness of the algorithm, all the results are averaged for 4000 Iteration. Computer Configurations used are Microsoft Windows 10, Intel i7 CPU 3 GHz, 8 GB RAM and Matlab 2022b. The encryption and decryption times are the time required by the algorithm to fully process a particular length of data is called the simulation time. It depends on the speed of the processor, the complexity of the algorithm, etc. The smallest value of the simulation time is required. The simulation times are calculated using a Matlab function called tic-toc.

4.1 Performance of U-ZUC and ZUC for 128-bit

In the two bars in Figure (4), the encryption and times of the proposed and ZUC algorithms are presented for ciphering 128-bit plaintext. It can be noticed that the proposed algorithm has encryption times less than the ZUC algorithm.

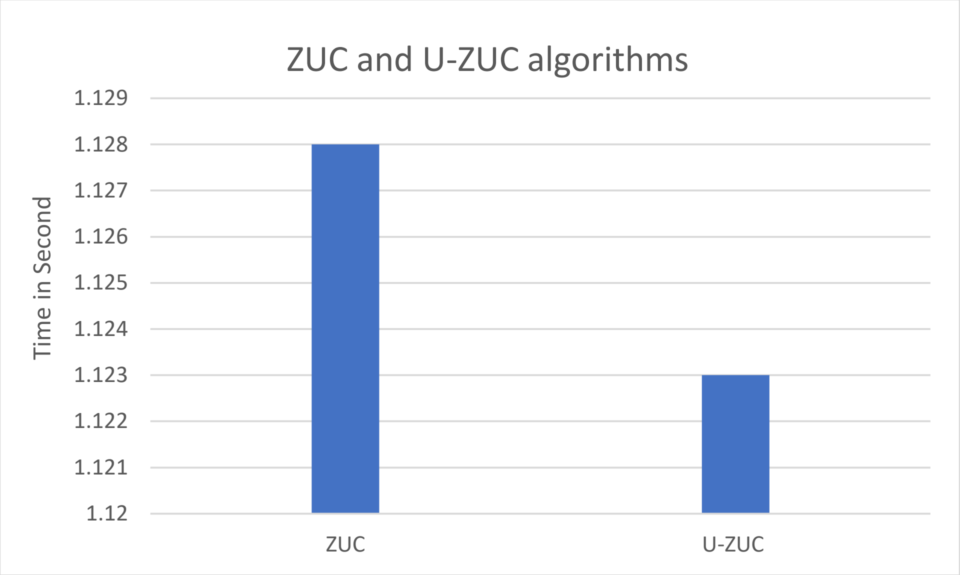

Figure (4): Encryption time Vs the U-ZUC and ZUC algorithms to encrypt 128-bit plaintext

The 128 bits test implementation of U-EEA3 to guarantee the encryption process is shown in Table (1). All input data enter the algorithm are binary. Hence, for the purpose of simplicity they are converted to Hexadecimal.

Table (1): Test Implementation of 128 bits U-EEA3

Plaintext:	935BC6FE03E5CE49581566B7C7441FEF
IV:	041073A4F8000000041073A4F8000000
CK:	B2CB8E97B8E252216D4A24C1D0038E61
Keystream:	8205A4D62252D5FE7E55CF4EEC314D578
Key M-EEA3:	4FAFF95A00B4664377E10B8578C235D1
Ciphertext:	FCAE72C6267CF7EDCAA899DC7C92FF46

4.2 Performance of U-EEA3 and EEA3 for 128-bit

In this section, the encryption and times of the two algorithms will be presented. The U-ZUC is the core of the U-EEA3 algorithm and the ZUC is the core of the EEA3 algorithm. The test in this part of simulation is to encrypt 128-bit plaintext. The two bars in Figure (5) shows the encryption times of the two algorithms respectively. It's obvious from the Figures, the U-EEA3 algorithm has less encryption and de-encryption times as compared with EEA3 algorithm.

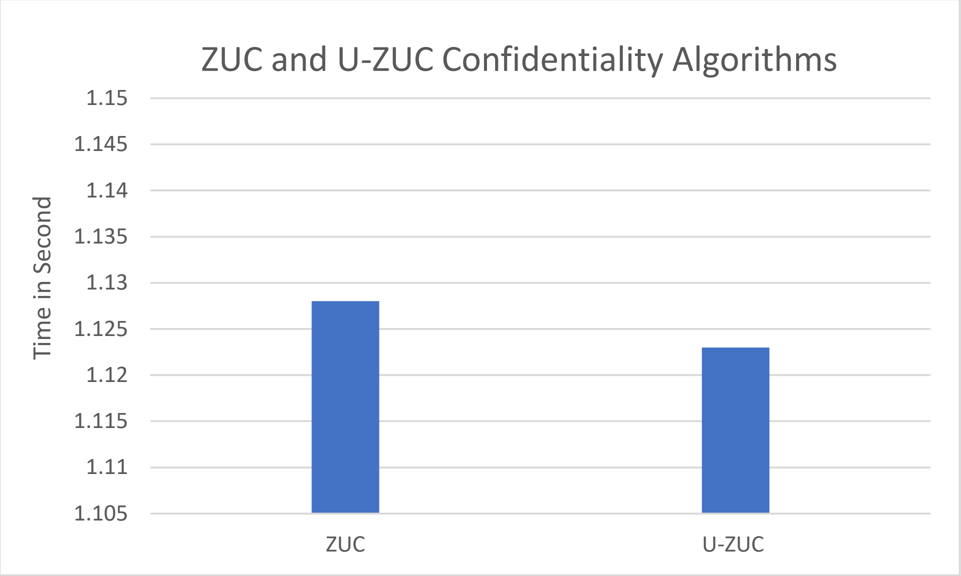

Figure (5): Encryption time Vs 128-EEA3 and the Proposed confidentiality Algorithm 128-M-EEA3

5. Conclusions

In this paper, the ZUC has been studied and analyzed to improve the security of 4th G mobile wireless system. Also, an upgrade has been done on ZUC algorithm to get a new version of ZUC algorithm that is we called U-ZUC. Also, the proposed U-ZUC is to be the core of the new version of EEA3 confidentiality algorithms; that we called U-EEA3 which also implemented and tested in this work. All the results we have been got seems a reduction in the encryption times. According to the obtained results, many points are concluded; the encryption times is reduced using the proposed algorithm, the security of the LTE system is enhanced and the storage space in the designing of the overall security system is reduced for further hardware implementation.

References

[1] Elias Bou Harb, *"A Distributed Architecture for Spam Mitigation on 4G Mobile Networks"*, September 2011.

[2] Ghizlane Orhanou , Saïd Elhajji , Youssef Bentaleb and Jalal Laassiri, *"EPS Confidentiality and Integrity mechanisms Algorithmic Approach "*, International Journal of Computer Science Issues, Vol. 7, Issue 4, No 4, July 2010.

[3] Christopher Cox ," *An Introduction to LTE, LTE-Advanced, SAE and 4G Mobile Communications"*, WILEY, first edition, 2012.

[4] Mr.Praneet R Shah and Prof.N.B.Hulle, *" Reconfigurable Hardware for ZUC Stream*

Cipher " ; International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, ISSN: 2277 128X, February 2014.

[5] Hai Cheng, Chunguang Huang, Qun Ding and Shu-Chuan Chu, *"An Efficient Image Encryption Scheme Based on ZUC Stream Cipher and Chaotic Logistic Map"*, Conference on Intelligent Data analysis and its Applications, Springer, Volume 2, 2014.

[6] Berad S. S. and Rahane S.B., " *An FPGA Implementation of ZUC Stream Cipher* ", International Journal of Engineering Research & Technology (IJERT), Vol. :2 Issue 12, December - 2013.

[7] Paris Kitsos, Nicolas Sklavos, George Provelengios and Athanassios N. Skodras, " *FPGA-based performance analysis of stream ciphers ZUC, Snow3g, Grain V1, Mickey V2, Trivium and E0* ", Microprocessors and Microsystems 37, 2013.

[8] Mayur Solanki, Seyedmohammad Salehi, and Amir Esmailpour ,*" LTE Security: Encryption Algorithm Enhancements "* , Norwich University, 2013 ASEE Northeast Section Conference , March 14-16, 2013.

[9] Assist. Prof. Dr. Natiq Abdullah Ali and Mays A. Anaee, "*A New Ciphering Algorithms for the 4th Generation Mobile System Based on ZUC Algorithm "* , 14th Conference of Scientific Research, at Al-Mansour University College from 25 to 26 April 2015.

[10] Vikas Kaula*, Bhushan Nemadeb, Dr. Vinayak Bharadic, Dr. S. K. Narayan khedkard, *Next Generation Encryption using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks*, 7th International Conference on Communication, Computing and Virtualization 2016.

[11] Zakaria Hassan Abdelwahab , Talaat A. Elgarf & Abdelhalim Zekry, *Approved algorithmic security enhancement of stream cipher for advanced mobile*, Information Security Journal: A Global Perspective, Published online: 17 Jun 2020.