مجلة الدراسات التربوية والعلمية - كلية التربية - الجامعة العراقية
العدد الثالث والعشرون - المجلد السادس - علوم الفيزياء - نيسان 2024م
doi.org/10.52866/esj.2023.06.23.08

Improvement of the ZUC 4th Mobile Security Algorithm Performance Based on Reducing the Number of Shift Registers in Bit-Reorganization Stage

Saba Abdulbaqi Salman
College of Education / AL-Iraqia University / Baghdad, Iraq

Abstract:

Due to extremely high demand of mobile phones among people, many Internet users use smart phones not only as a means of communication, but also as a way to organize work and monitor the progress of work and special services, that means all smart phones and computers are used to transfer important information, and especially, such as Messages. (SMS), (MMS).... etc., therefore they must provide various applications and security services for protecting information and the communication.

Long Term Evolution is one of the mobile systems that used in Fourth Generation (4thG) cellular networks. Long Term Evolution (LTE) is a modern and newest technology that is emerged to improve the security and service of communication. Also, it has many features that make them compete with other technologies in network of mobile, LTE provides users with many applications with high experience, these applications are such as video generator programs, games, interactive TV and professional services.... etc.

In this work is an attempt to study the LTE security and dealing it with stream cipher algorithm which is called ZUC algorithm. In this paper, we proposed a modified version of Zu-Chongzhi (ZUC) ciphering algorithm to decrease encryption time and enhance security. MATLAB software ver. 2013a is used in this work for the proposed algorithms.

Keyword: ZUC algorithm, Mobile security, Shift registers in digital logic.

تحسين أداء خوارزمية الأمان المتنقلة الرابعة لـ ZUC بناءً على تقليل عدد سجلات التحول في مرحلة إعادة تنظيم البت

صبا عبد الباقي سلمان
كلية التربية / الجامعة العراقية / بغداد، العراق

مستخلص:

هناك ارتفاع كبير على طلب الهواتف النقالة بين الناس نتيجة لازدياد عدد مستخدمي الانترنت ومستخدمي الهواتف الذكية ليس كوسيلة اتصال فقط ولكن ايضا تم استخدامها كوسيلة لتخطيط وتنظيم عملهم وحياتهم الخاصة وهذا يعني أن جميع الهواتف الذكية واجهزة الكمبيوتر تستخدم لنقل المعلومات الهامة وخاصة مثل الرسائل القصيرة ورسائل متعددة الوسائط ..... الخ، لذلك يجب توفير مختلف التطبيقات والخدمات الأمنية لحماية المعلومات والاتصالات.

التطور طويل الأمد هو واحد من الانظمة المتنقلة التي تستخدم في الجيل الرابع من الشبكات الخلوية. تطور طويل الأمد هي تقنية حديثة ظهرت لتحسين امن وخدمة الاتصالات ايضا كان لديه العديد من المميزات التي تجعلها تنافس مع غيرها من التقنيات الأخرى في شبكة الهاتف المحمول، حيث توفر هذه التقنية للمستخدمين العديد من التطبيقات ذات الخبرة العالية، وهذه التطبيقات مثل برامج الفيديو والالعاب والتلفزيون التفاعلي والخدمات المهنية .

في هذا البحث سيتم دراسة امنية تقنية التطور طويل الأمد وتحديدا للجيل الرابع والتعامل مع تيار خوارزمية التشفير وهذه الخوارزمية تدعى ZUC . تعتبر هذه الخوارزمية محور العمل في هذا البحث وايضا تعد بانها قلب الخوارزمية السرية. في هذا البحث اقترحنا نسخة معدلة من خوارزمية الـ ZUC لتقليل وقت التشفير وتعزيز الأمن تم استخدام برنامج الماتلاب الاصدار 2013 في هذا العمل.

الكلمات المفتاحية: خوارزمية ZUC، أمن الهاتف المحمول، مسجلات Shift في المنطق الرقمي.

1. Introduction

The motivation behind LTE security is to give an intense safeguard instrument against conceivable dangers from the web forced by different sorts of assaults [1]. Protection the information is very important feature in 4G mobile system. Where developed the cryptology over the centuries from an art, we have several goals to achieve the security professionals via utilize of cipher. These objectives incorporate privacy, element validation, information honesty, non-disavowal and information beginning verification. The Cipher includes two linked fields: cryptanalysis and cryptography. The technique of analyzing and break, security of the information called Cryptanalysis. Also, the mathematics technique which is used to guarantee different parts of data security called cryptography [2 and 3].

There are two of standard schemes namely EPS Integrity Algorithm (EIA) and EPS Encryption Algorithm (EEA). Have already been identified confidentiality and integrity algorithm. The principal group. 128-EEAI and 128-EIAI, depends on the stream cipher SNOW 3 generation. The next group, 128-EEA2 and 128-EIA2, depends on a block cipher Advanced Encryption Standard (AES). The third group. 128-EEA3 and 128-EIA3, composed in China, the subsequent scheme set depends on a center stream cipher scheme called ZUC, by Zu-Chongzhi, the popular Chinese researcher [4].

In this work, we proposed an algorithm by modifying the ZUC. The MATLAB (2013a) was used in the simulation of this work and the also the obtained results.

2. ZUC Algorithm

The cipher system is generally divided into stream cipher and block cipher. The stream cipher works on singular character of the plaintext data into a period [5]. Then the block cipher works to encrypt sets of characters at a time. A ZUC Algorithm is one of the streams (ciphers are the word-oriented stream ciphers). Figure (1) shows a structure of ZUC algorithm [6].

This algorithm picks (128 bit) as starting key with (128 bit) as starting vector and the output is (32 bit) word as a key-stream that is utilized for encrypting and decrypting data. When implement ZUC scheme there are two phases as follow: first phase called initialization which is performs keys, parameters and procedures. Second phase called working that run algorithm processes with (32 bit) word as output per circle with each pulse [7].

As per a ZUC detail [8], it is made out of three reasonable layers. The upper layer is a Linear Feedback Shift Register (LFSR) of 16 phases: then a center layer called a bit reorganization (BR) methodology, and a base layer is a Function namely (F) process.

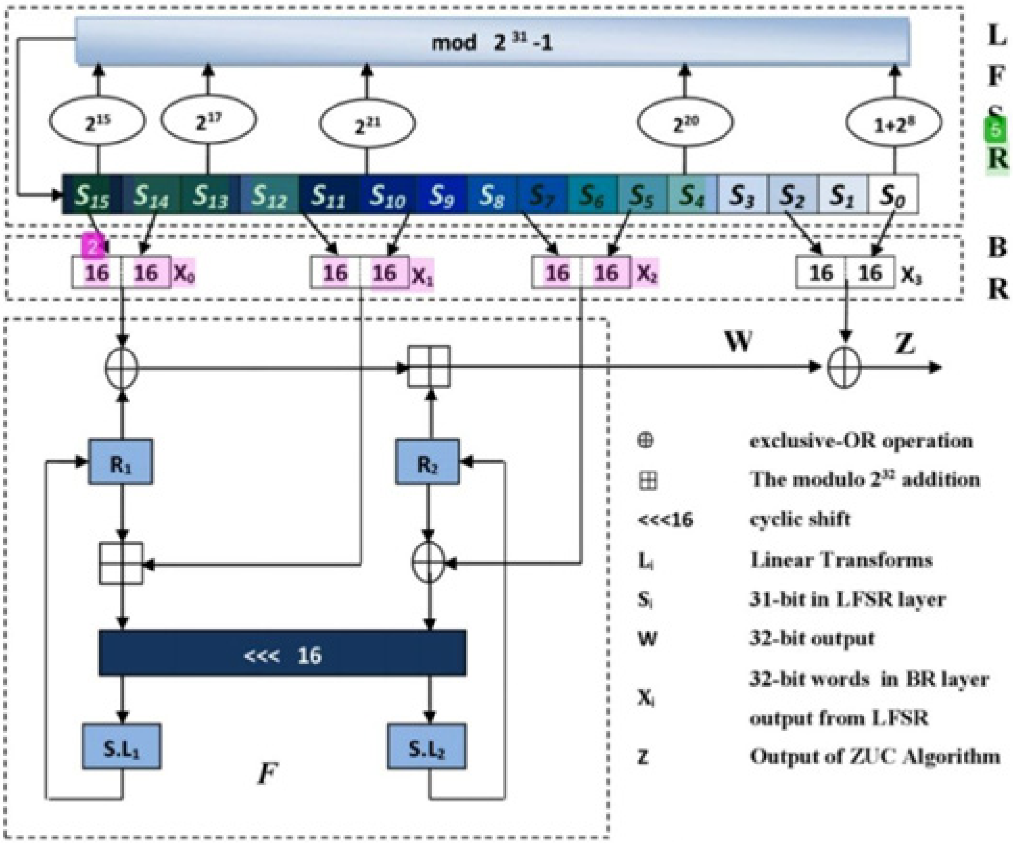
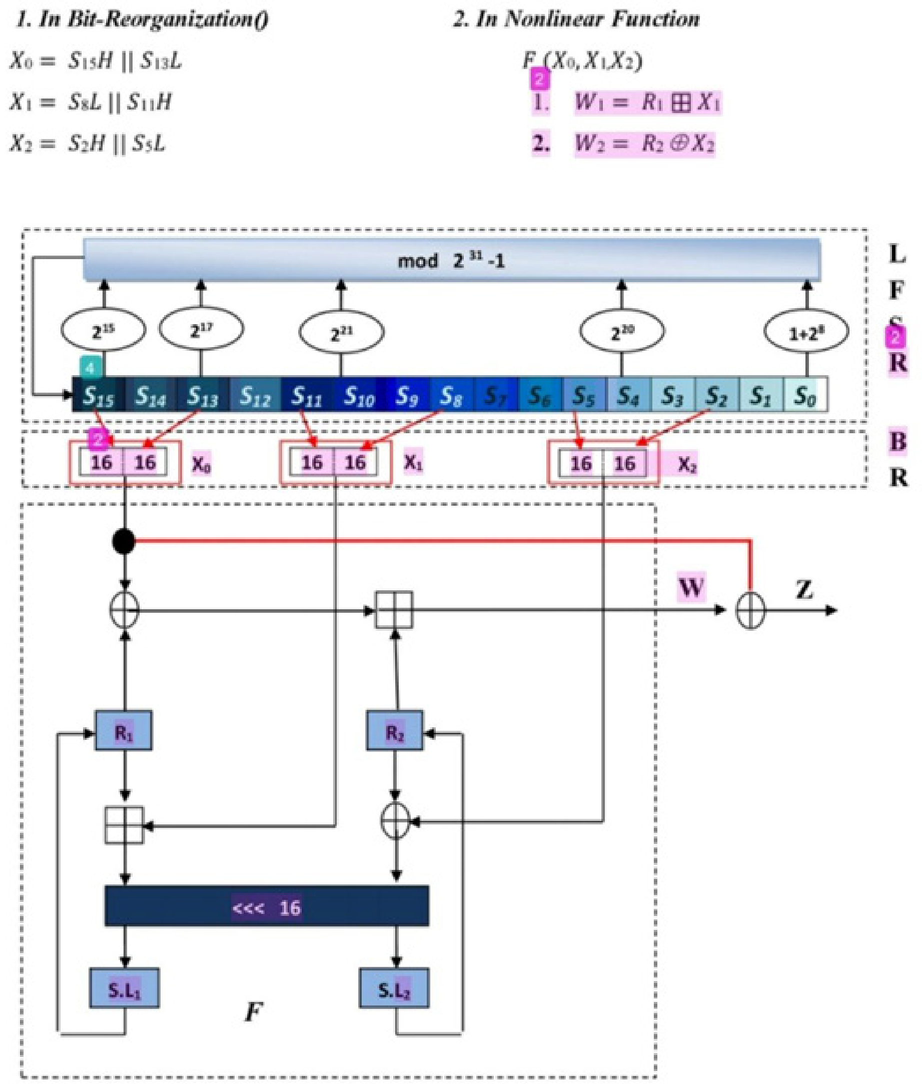

mod 2^{31}-1
2^{15}
2^{17}
2^{21}
2^{20}
$1+2^{8}$
LFSR
S_{15} S_{14} S_{13} S_{12} S_{11} S_{10} S_9 S_8 S_7 S_6 S_5 S_4 S_3 S_2 S_1 S_0
16 16 X_0
16 16 X_1
16 16 X_2
16 16 X_3
BR
W
Z
R_1
R_2
<<< 16
$S.L_1$
$S.L_2$
F
⊕ exclusive-OR operation
⊞ The modulo 2^{32} addition
<<<16 cyclic shift
L_i Linear Transforms
S_i 31-bit in LFSR layer
W 32-bit output
X_i 32-bit words in BR layer output from LFSR
Z Output of ZUC Algorithm

Figure (3): The ZUC algorithm structure [6]

3. The Proposed ZUC Algorithm

This work proposed a new ZUC algorithm. In the next two sub-sections, a detailed description of this proposed algorithm is presented.

This algorithm that contains some changes in the two layers (BR layer and F layer). In BR layer, words will be reduced from four to three words, this step also reduces storage space when reducing the number of words. In the F layer, there is a simple change that is when using (Xo) in more than way, that means using (Xo) to find the result of (W) and also using it to find (Z) as shown in Figure (2). The changes in the equations are as follow:



1. In Bit-Reorganization()

$X_0 = S_{15}H \,||\, S_{13}L$

$X_1 = S_8L \,||\, S_{11}H$

$X_2 = S_2H \,||\, S_5L$

2. In Nonlinear Function

$F(X_0, X_1 X_2)$

1. $W_1 = R_1 \boxplus X_1$
2. $W_2 = R_2 \oplus X_2$

Figure (2): The proposed ZUC algorithm

4. The Results and Discussion

In this paper, we proposed ZUC algorithm that uses with 4G mobile syṡtem. The proposed algorithm is increasing the security of the 4G and reducing the time of encryption and decreeing ṡtorage space. The main aims of this proposed algorithm to increase the security to protect all information text, image, video, e-mail.

In graph below we can show differences among the algorithms (The original ZUC, and the proposed ZUC) according to the encryption time.

The encryption time of the two algorithms are around shown in Figure (3). This is due to the randomness of the algorithms. Hence, we are forced to implement the two algorithms rounding to this issue. We can see the differences in encryption time of the two algorithms when ciphering a 128-bit plain text. Also, from the graph, we notice that the time encryption of the ZUC algorithm “The original one” is around (1.0273 sec.) and for the proposed algorithm is around (1.0261 sec.), the encryption times are less than ZUC algorithm. That is mean that the proposed algorithm is best in encryption time also reducing storage space with high security.

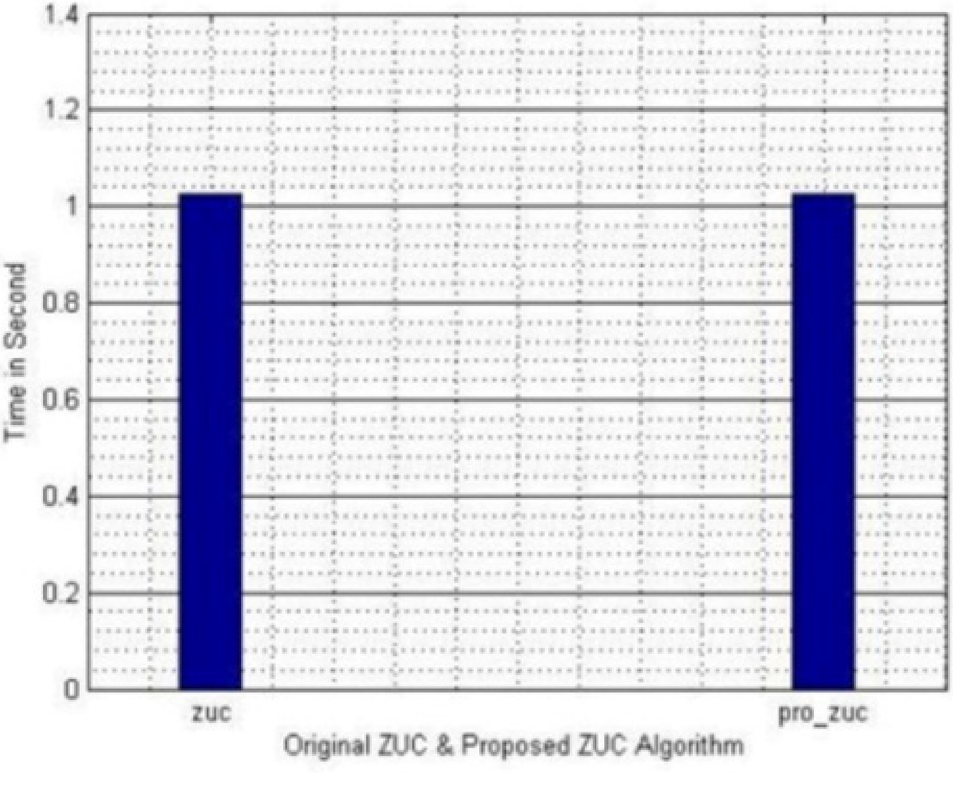


Figure (3): Encryption time Vs Cipher Algorithm: ZUC algorithm and the proposed algorithm for encryption 128 bit

5. Conclusions

This paper presents an investigation of a novel LTE privacy algorithm M-EEA3 in view of a stream cipher ZUC scheme then proposed ZUC algorithm that uses in 4G mobile system.

According to the obtained result, many points are calculated. First, the encryption time is reduced. Second, the security of the LTE is enhanced. Third, the storage space is reduced for further hardware implementation of the proposed system.

References

[1] Mayur Solanki, Seyed mohammad Salehi, and Amir Esmailpour; "LTE Security: Encryption Algorithm Enhancements": 2013 ASEE Northeast Section Reviewed Paper Conference Norwich University: March 14-16, 2013.

[2] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, "Handbook of Applied Cryptography". CRC Press. 5th edition, 2001.

[3] Leglise, P. Standaert. F. Rouvroy, G., Quisquater," Efficient implementation of recent stream ciphers on reconfigurable hardware devices ": In: 26th Symposium on Information Theory in the Benelux, pp. 261-268 (2005).

[4] ETSI/SAGE, "Specification of the 3GPP Confidentiality and Integrity Algorithms 128EEA3 & 128-EIA3. Document 2: ZUC Specification"; Version 1.6, 28th June, 2011(Published in 2012).

[5] Louay A Hussein Al-Nuamy, "Enhance LFSR Cipher". European Journal of Advances in Engineering and Technology. ISSN: 2394 - 658X, 2015.

[6] 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 4: Design and Evaluation Report, version 2.0, 9th September 2011.

[7] 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.2014 ,2

[8] 3GPP Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS); Stage 3Release 10, 3GPP Technical Specification 24.301, version 10.4.0, September 2011.