Overview of ZUC Algorithm and its Contributions on the Security Success and Vulnerabilities of 4G Mobile Communication

Alyaa Ghanim Sulaiman
Department of Software Engineering,
College of Mathematical & Computer Science,
University of Mosul, Iraq

ABSTRACT
With tremendous challenges in mobile communication toward a very advanced security level against new threats, ZUC algorithm emerged to overpass various algorithms that common before. ZUC is a stream cipher which is the core of the both newly LTE algorithms (LTE encryption and integrity algorithms). Nowadays, a mobile has been a crucial thing in people's daily life and people used to save their information including personal information on it. In addition, the accelerated change in mobile generations requires an appropriate algorithm to cope with the change and achieve more security demands. Therefore, Chinese cryptography experts have been designed ZUC algorithm to cope with 4G mobile security to overcome the obstacles that the previous generation had before with a flexibility to develop and change. The purpose of this research is to provide an extensive study on the ZUC algorithm and show the improvements that have been done till now and the vulnerabilities of the ZUC algorithm against different attacks.

Keywords
4G/ LTE, ZUC, improvements, vulnerabilities.

1. INTRODUCTION
Based on ABI research estimation [25], the 4G/LTE subscribers are growing up during the last three years and it is estimated to hit or exceed 3.5 billion by 2020. In addition, it is expected to expand by 10% year by year. From this point of view, the significant of 4G/LTE is crucial in our daily life and the aspect of security should be constrained from the experts and researchers to achieve high level of security and throughput. LTE is a candidate for a project of 3GPP (3rd Generation Partnership Project).The growing demands on mobile services have encouraged many researchers toward achieving multi- services with low latency. To illustrate that, Lingchen Zhang in 2012 [10] pointed out the LTE (Long Term Evolution) is a standard for high-speed wireless data communications which is maintained as a project of the 3rd Generation Partnership Project (3GPP). In addition, to cover the requirements of the mobile migrations of Internet applications, such as VOIP, video streaming, music downloading and mobile TV, LTE networks offer the capacity to tolerate the throughput explosion for the connection from mobile devices customized to those new mobile applications. However, the standardized cryptographic algorithms provide 4G/LTE security architecture with multi services, which are necessary for the radio interface. In particular, they support LTE security with two standardized algorithms EEA (Encryption algorithm), EIA (Integrity algorithm). [2]

In fact, the two encryption and integrity algorithm sets have already been developed and standardized for LTE. The first set, 128-EEA1 and 128-EIA1, is based on SNOW 3G; the second, 128-EEA2 and 128-EIA2, is based on AES. (The prefix "128-" indicates that the algorithms take a 128-bit secret key.) In May 2009, [12][4] 3GPP SA3 agreed on the needs of a third encryption and integrity algorithm set which designed in China so that the Chinese authorities would not permit its use in other countries. The resulting algorithms (128-EEA3 and 128-EIA3) based on stream cipher called" ZUC", the name derived from Zu Chongzhi, the famous Chinese scientist from history. The algorithms were designed by experts at the Data Assurance and Communication Security Research Center (DACAS) of the Chinese Academy of Sciences but "an algorithm from China" is not enough of a requirement. It was agreed that a robust, three-phase evaluation program would be followed

- Evaluation by an ETSI SAGE task force;
- Evaluation by two funded teams of academic experts, delivering their results [4] to the ETSI SAGE task force;
- After that evaluation, if the task force recommended that the algorithm (modified or not) is suitable for acceptance into the standard, then a public evaluation phase would take place before final standardization. Therefore, in this paper we first present an overview on ZUC algorithm and then highlight the present works or researches that improve the security of ZUC algorithm from software and hardware perspectives and then we show the vulnerability of ZUC algorithm against different attacks.

2. OVERVIEW OF THE ZUC ALGORITHM
ZUC is a word-oriented stream cipher [3].It takes a 128-bit initial key and a 128-bit initial vector as input, and outputs a keystream of 32-bit words, which is used to encrypt/decrypt the plain/encrypted data shown Fig1.

There are two stages in the execution of ZUC: 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.

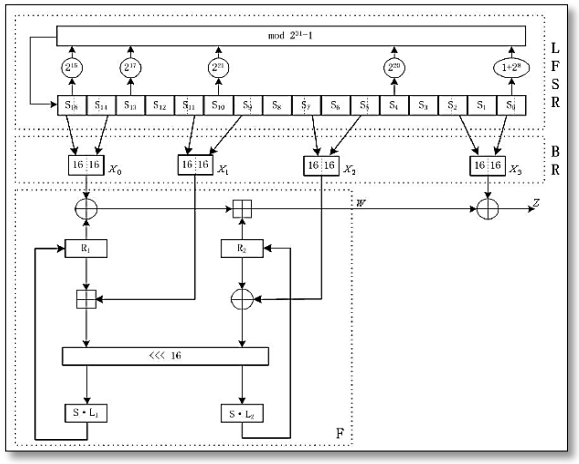

Fig 1. ZUC algorithm architecture.

According to the ZUC specification [3][4], ZUC is composed of three logical layers. The top layer is a linear feedback shift register (LFSR) of 16 stages; the middle layer is bit-reorganization (BR) procedure, and the bottom layer is a nonlinear function *F* procedure.

2.1. The Linear Feedback Shift Register (LFSR)

The linear feedback shift register (LFSR) has 16 of 31-bit registers (*S*0, *S*1,..., *S15*). Each register *Si*(0 >= *i* <= 15) is restricted to take values from the following set: {1, 2, 3, . . . , 2^31 − 1}. The LFSR has two modes of operations: the initialization mode and working mode. The initialization mode works as Algorithm 1 shown below. [7][4]

Input: *u*
1 begin
2 $v = \{2^{15}S15 + 2^{17}S13 + 2^{21}S10 + 2^{20}S4 + (1 + 2^8)\ S0\} \bmod (2^{31} - 1)$;
3 $S16 = (v + u) \bmod (2^{31} - 1)$;
4 if $S16 = 0$ **then**
5 set $S16 = 2^{31} - 1$
6 $(S1, S2, \ldots, S15, S16) \rightarrow (S0, S1, \ldots, S14, S15)$;

Algorithm 1. LFSR with Initialization Mode.

In the working mode, the LFSR does not receive any input; the LFSR works independently with other parts of ZUC, which inspires us that if we acquire *S*16 per clock pulse, the shift registers perform shifts per clock cycle, meaning that we generate a 32-bit key every clock cycle as shown in Algorithm 2. [7]

begin
$S16 = \{2^{15}S15 + 2^{17}S13 + 2^{21}S10 + 2^{20}S4 + (1+2^8)S0\} \bmod (2^{31} - 1)$;
if $S16 = 0$ **then**
set $S16 = 2^{31} - 1$
$(S1, S2, \ldots, S15, S16) \rightarrow (S0, S1, \ldots, S14, S15)$;

Algorithm 2. LFSR With Work Mode. [7]

2.2.The Bit-Reorganization (BR)

The middle layer of ZUC is the bit-reorganization (BR) procedure. Supposing that *S*0, *S*2, *S*5, *S*7, *S*9, *S*11, *S*14 and *S*15 are eight registers of LFSR. Then the BR forms four 32-bit words *X*0, *X*1, *X*2 and *X*3 in accordance with Algorithm 3, and the first three words are passed to the next bottom layer, nonlinear function *F*. More detailed description can be found in [3]. Compared with software implementations, to realize the concatenation of signals in hardware, we only need to change the wires order, and it hardly costs any time to complete this. Therefore, BR procedure should mix with the nonlinear function *F* operation together to save clock cycles.

Begin
X0 = S15H ||S14L;
X1 = S11L ||S9H;
X2 = S7L ||S5H;
X3 = S2L ||S0H;

Algorithm 3. Bit-Reorganization (BR)

2.3. The Nonlinear Function *F*

There are two 32-bit memory cells, *R*1 and *R*2, in the nonlinear function *F* procedure. The input of *F* is *X*0, *X*1 and *X*2, which are the first three words of output of BR procedure, and it outputs a 32-bit word *W*. The detailed process of the nonlinear function *F* is described in Algorithm 4.
In Algorithm 4, *S* is a 32 × 32 S-box; *L*1 and *L*2 are linear transformations, which are defined as Equation (1) and (2) respectively as shown in Figure 2.

$$L1(X) = X \oplus (X \lll_{32} 2) \oplus (X \lll_{32} 10) \oplus (X \lll_{32} 18) \oplus (X \lll_{32} 24) \quad (1)$$
$$L2(X) = X \oplus (X \lll_{32} 8) \oplus (X \lll_{32} 14) \oplus (X \lll_{32} 22) \oplus (X \lll_{32} 30) \quad (2)$$

Fig 2. Equation (1) and (2).

In the nonlinear function *F* stage, the critical path is the calculation of $W1 = R1 \boxplus X1$, where $\boxplus$ denotes the modulo 2^{32} addition. Compared with the modulo addition, the other operations in nonlinear function *F* cost negligible time as shown in Algorithm 4.

Input: *X*0,*X*1,*X*2
1 Begin
2 $W = (X0 \oplus R1) \boxplus R2$;
3 $W1 = R1 \boxplus X1$;
4 $W2 = R2 \oplus X2$;
5 $R1 = S(L1(W1L \ \|W2H))$;
6 $R2 = S(L2(W2L \ \|W1H))$;

Algorithm 4. The Nonlinear Function *F*.

So, we assume that the nonlinear function *F* and bit reorganization operation can be done in one clock cycle, that is to say, if LFSR complete the update every clock cycle, ZUC is able to generate a 32-bit key per clock cycle. [7][8]

2.4. The Key loading

The key loading procedure will expand the initial key and the initial vector into 16 (31-bit) integers as the initial state of the LFSR. Let the 128-bit initial key and the 128-bit initial vector IV be K=K0||K1||K2||…..||K15 and IV=IV0||IV1||IV2||….||IV15 separately, where Ki and IVi , are all bytes. Then Ki and IVi are loaded into the cells Si as Si=Ki||Di||IVi, where Di is a known constant. [8]

2.5. The Execution of ZUC

The execution of ZUC is composed of two stages: the initialization stage and working stage. During the initialization stage, the cipher algorithm runs the following operations 32 times to finish the initialization:

1. Bitreorganization();
2. $w = F(X0,X1,X2)$;
3. *LFSRWithInitialisationMode*($w>>1$);

After the initialization stage, the algorithm moves into the working stage. At the beginning of this stage, the algorithm executes the following operations once, and discards the output W of nonlinear function F:

1. Bitreorganization();
2. $F(X0,X1,X2)$;
3. *LFSRWithWorkMode*();

Then the algorithm goes into the stage of producing keystream, i.e., for each iteration the following operations are executed once, and a 32-bit word Z is produced as an output:

1. Bitreorganization();
2. $Z = F(X0,X1,X2) \oplus X3$;
3. *LFSRWithWorkMode*();

3. SUCCESSFUL IMPROVEMENT OF ZUC ALGORITHM

Several researches from 2011 till now tried to enhance and empower the security of ZUC algorithm. Therefore, this section presents the contributions have been done to improve the efficiency of ZUC cryptographic algorithm some by optimizing the structure of ZUC or some by modifying the algorithm itself to obtain high throughput with less consumed area. The literature survey on enhancing ZUC algorithm presented in Table1 below.

Table 1. Literature survey on enhancing the ZUC algorithm.

Year	Authors	Contribution
2011	Lei Wang	Proposed in his paper three optimized schemes to implement ZUC and he made a comparison among them in terms of both performances and consumed area in FPGA environment.[7]
2011	Sourav Sen Gupta	Designed HIPACC-LTE for SNOW 3G and ZUC (version 1.5, as in LTE Release 10 and beyond), targeted towards the 4G mobile broadband market.[5]
2012	Ghizlane Orhanoun et al.	Studied the internal structure of ZUC and how it works. Moreover, he constrained on giving a clear image of the time and space complexity of the ZUC during its modes.[26]
2012	Shadi Traboulsi et al.	Designed and analyzed various architectures in order to reduce the using of power and area of ZUC algorithm. [15]
2013	Zongbin Liu	Proposed a novel mixed two stages pipeline architecture of ZUC in order to significantly increase the ratio of the throughput of ZUC in hardware and he implemented it on FPGA and ASIC. [6]
2013	Anastasios N. Bikos	Figured out some advantages of ZUC algorithm such as: 1) Meeting the requirements of the 3G security environment. 2) Provide strong encryption via 128-bit keys. 3) It appeared to have a sound design with a large security spectrum and builds on design principles of well-known ciphering algorithms. [14] 4)Another advantage, the official design and evaluation report [13] gave the evaluation of the ZUC algorithm on the resistance against several cryptanalytic attacks, weak key attacks, guess-and-determine attacks, algebraic attacks, fast correlation attacks and linear distinguishing attacks, timing attacks. [8]
2014	Sulabh Bhattarai et al.	Have done a framework for exploring modern attacks on 4G/LTE technology via regularly reconnoitering the attack space. [16]
2014	Shri Ramtej et al.	Modified EEA3 algorithm which is a confidentiality algorithm based on ZUC cryptographic algorithm. So, this modification improved the performance of the EEA3 which decreased the encryption time of the message.[18]
2014	Jin Cao et al.	made contributions on the LTE and LTE-A network security. They show an overview of the security functionality for both LTE and LTE-A. Next, they presented the vulnerabilities that exists in the security architecture of the LTE and LTE-A. Then, they overviewed of the current solution to the existing problems and showed some issues for future works. [20]
2014	Khalid Fadhil et al.	did a comparative study among the symmetric cryptographic algorithms of LTE technology in order to highlight the vulnerabilities of security issue which exist in these algorithms and also illustrated some of the cryptanalysis methods that can be used to attack the current LTE symmetric cryptographic algorithms.[24]
2016	Aiqing Zhang et al.	proposed a secure data sharing protocol, which merges the advantages of public key cryptography and symmetric encryption, to achieve data security in D2D communication.[23]

2016	Zou et al.	pointed a survey study on the challenges of the wireless network security and the resisting mechanisms from malicious attack which is threaten the confidentiality, integrity and the availability of transmitting data across the wireless network including the LTE. [19]
2016	Maria Falaq et al.	implemented an exhaustive simulation for ZUC algorithm in hardware platform as FPGA and coded to C programming language and lastly converted to Verilog HDL.[21]
2016	Zongbin Liu et al.	proposed a new design for ZUC algorithm by optimizing the ZUC to working stage only which increased the throughput to the highest level estimated by 45% compared by previous design of ZUC. At the same time, the new design of ZUC saved the resources area by 12% .The new architecture of ZUC used FPGAs and ASICs platform. [22]

4. VULNERABILITY OF ZUC ALGORITHM

During study many researches, it can be noticed that there are some weaknesses or vulnerability in ZUC algorithm and they are abbreviated in the following points:

1) TANG Ming and CHENG PingPan in 2012, pointed out in their article there is a vulnerability of ZUC algorithm on DPA (Differential Power Analysis) attacks, their results based on theoretical analysis and experiments. For more detail refer to [8][28].

2) In addition, based on Anastasios N. Bikos during 2013, pointed that ZUC algorithm requires more analysis to gain further confidence. [14]

3) Stream cipher ZUC is weak against chosen IV attack [16][27]

Furthermore, the following Table 2 summarized the recent contributions on detecting the vulnerability of ZUC algorithm in LTE network.

Table 2. Vulnerability of ZUC algorithm

Year	Author	Contribution
2010	N. Seddigh & et al.	Pointed a set of potential LTE vulnerabilities at the MAC layer. For example, illegal use of user and mobile equipment, location tracking, DoS attacks and data integrity attacks.
2012	Ramsi Bassil	Showed a study of a denial of service (DOS) oriented signaling attack against LTE networks that takes advantage of the signaling overhead required to setup dedicated radio bearers. The attack scenario is simulated in OPNET and signaling traces are analyzed.
2013	Ramzi Bassil & et al.	Described a signaling attack that aims to increasing the volume of signaling traffic.
2013	Roger Pigueras	Overviewed of the current threat land space against the availability of LTE mobility of networks.
2014	Roger Pigueras & et al.	Overviewed a series of simple but effective jamming attacks that extend the range of basic jamming while requiring less power. he proposed a series of potential security research directions that could protect LTE cellular networks, forcing a potential attack to rely on just basic jamming to attempt a DOS charge.
2014	Sulabh Battarai	Developed theoretical framework to regularly explore the new attacks on LTE network through detecting the attack space.
2014	Alyaa Ghanim & et al.	Stated some weaknesses of ZUC algorithm against DPA attack. In addition, the work compared the three types of cryptographic algorithms based on different factors.
2015	Zoya Dyka & et al.	Presented a novel approach to prevent Side Channel Attack or at least to increase the effort to reveal keys significantly. Our approach is based on the fact that there are some functions used in cryptographic operations that can be implemented using different formulae or algorithms.

4. CONCLUSION

In a nutshell, from studying ZUC algorithm, it can be say that ZUC cipher is the robust stream algorithm that resists many different attacks and has a flexibility to do improvement to get higher performance and higher throughput than pervious works. Furthermore, there are some vulnerability still exist in ZUC algorithm and need to improve. Hence, this topic needs more search in the future to resist any new attack occur on mobile security. Some suggestions for future work, combining the benefits of block cipher and stream cipher to produce a new mixing algorithm, where the benefit of block cipher is using both small and large messages by having only one shared parameter and shared the symmetric key, while the benefit of stream cipher is encrypting or decrypting the messages with various keys and makes the attacks more complex. Furthermore, generate sub keys for each plaintext is making attacks impossible.

5. REFERENCES

[1] ETSI/SAGE Specification,"Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 1: ZUC Specification version: 1.6," 2011.

[2] ETSI/SAGE Specification "Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3.Document 2: 128-EEA3 and 128-EIA3 Specificationversion: 1.6," 2011.

[3] ETSI/SAGE Specification "Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3.Document 3: Implementors Test Data version: 1.6," 2011.

[4] ETSI/SAGE Specification "Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 4:Design and Evaluation Report version: 1.6," 2011.

[5] S. S. Gupta, A. Chattopadhyay, and A. Khalid, "Designing integrated accelerator for stream ciphers with structural similarities," Cryptography and Communications, vol. 5, no. 1, pp. 19–47, 2011.

[6] Zongbin Liu1, N. G., Jiwu Jing1, and Peng Liu2 (2013). "HPAZ: a High-throughput Pipeline Architecture of ZUC in Hardware."

[7] L. Wang, J. Jing, Z. Liu, L. Zhang, and W. Pan, "Evaluating Optimized Implementations of Stream Cipher ZUC Algorithm on FPGA," Information and Communications Security, pp. 202–215, 2011.

[8] TANG Ming1, CHENG PingPan2 ,QIU ZhenLong2 (2012). "Differential Power Analysis on ZUC Algorithm."

[9] Maitra, S. Evolution of Stream Ciphers towards ZUC, Indian Statistics Unit.

[10] Lingchen Zhang, L. X., Zongbin Liu, Jiwu Jing and Yuan Ma (2012). "Evaluating the Optimized Implementations of SNOW3G and ZUC on FPGA". IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[11] Sourav Sen Gupta, A. C., Ayesha Khalid (2011). "HiPAcc-LTE: An Integrated High Performance Accelerator for 3GPP LTE Stream Ciphers."

[12] El-Hajji, G. O. a. S. (2013). "The New LTE Cryptographic Algorithms EEA3 and EIA3 Verification, Implementation and Analytical Evaluation."

[13] ETSI/SAGE Specification "Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 4: Design and Evaluation Report", Version: 2.0 (September 9, 2011).

[14] Anastasios N. Bikos, N. S. (April 2013). "LTE/SAE Security Issues on 4G Wireless Networks." IEEE Computer and Reliability Societies".

[15] Traboulsi, S., Pohl, N., Hausner, J., Bilgic, A., & Frascolla, V. (2012, February). Power analysis and optimization of the ZUC stream cipher for LTE-advanced mobile terminals. In Circuits and Systems (LASCAS), 2012 IEEE Third Latin American Symposium on (pp. 1-4). IEEE.

[16] Wu, H., Nguyen, P. H., Wang, H., & Ling, S. (2010). Cryptanalysis of the stream cipher zuc in the 3gpp confidentiality & integrity algorithms 128-eea3 & 128-eia3. Rump session of Asiacrypt, 2010.

[17] G.Orhanou, S. EI Hajii, "Analytical Evaluation of the stream cipher ZUC", IEEE, 2012.

[18] Kondamuri, S. R., Gupta, N. K., & Sharma, R. (2014, July). Modified EEA3 algorithm with improved throughput performance. In Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on (pp. 890-894). IEEE.

[19] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE, 104(9), 1727-1765.

[20] Cao, J., Ma, M., Li, H., Zhang, Y., & Luo, Z. (2014). A survey on security aspects for LTE and LTE-A networks. IEEE Communications Surveys & Tutorials, 16(1), 283-302.

[21] Maria Falaq, Dr. Syed Abdulhayan "LTE Security: EEA 3 using ZUC Algorithm", IJIRCCE Journal, Vol.4, Issues 7, July 2016.

[22] Liu, Z., Zhang, Q., Ma, C., Li, C., & Jing, J. (2016, March). HPAZ: a High-throughput Pipeline Architecture of ZUC in Hardware. In Design, Automation & Test in Europe Conference & Exhibition (DATE), 2016 (pp. 269-272). IEEE.

[23] Zhang, A., Chen, J., Hu, R. Q., & Qian, Y. (2016). SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks. IEEE Transactions on Vehicular Technology, 65(4), 2659-2672.

[24] Jasim, K. F., & Al Shaikhli, I. F. (2014, November). Comparative study of some symmetric ciphers in mobile systems. In Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on (pp. 1-5). IEEE.

[25] Research, A. (2015). "LTE Subscriber Base to Grow to 1.4 Billion Globally by Year-end 2015." from https://www.abiresearch.com/press/lte-subscriber-base-to-grow-to-14-billion-globally/.

[26] Orhanou, G., El Hajji, S., Lakbabi, A., & Bentaleb, Y. (2012, May). Analytical evaluation of the stream cipher ZUC. In Multimedia Computing and Systems (ICMCS), 2012 International Conference on (pp. 927-930). IEEE.

[27] Ghanim, A., & Alshaikhli, I. F. T. (2014). Comparative study on 4G/LTE cryptographic algorithms based on different factors. International Journal of Computer Science and Telecommunications, 5(7), 7-10.

[28] Sulaiman, A. G. (2014). Comparative Study On 4g/Lte Network Security Algorithms. Information Technology. Malaysia, IIUM.