International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-7)

Research Article

July 2017

Review on LTE Cryptography Algorithm ZUC and its Attacks

Saurabh Lawange[1], Manish Narnaware[2]
[1]Student, Dept. of Information Technology, WCE, Sangli, India
[2]Assistant Professor, Dept. of Information Technology, WCE, Sangli, India

Abstract:

Security is the important when it comes to wireless communication, and as the expectations of people increased, the data service now arrived at LTE. The faster data access and communication with high priority security. ZUC is the algorithm adopted to provide security under third set of LTE i.e. EEA3 and EIA3. The algorithms are used for confidentiality and integrity protection over the air. To analyze the security level of the algorithm different attacks were published in literature. The aim of this paper is to discuss the working of ZUC algorithm in detail. Also different attacks are listed in the last section.

Keywords: LTE; ZUC; Cryptanalysis; SAT; Chosen IV; TMTO

I. INTRODUCTION

The data and voice communication happens over the air thus security algorithms were introduced. As the stream ciphers are computationally efficient, stream ciphers are preferred over block ciphers for security. For the GSM, A5 family of algorithms are used, for 3G KASUMI, SNOW 3G are used. As the algorithms were analyzed, the need for more efficient security algorithm is arrived. Cellular technology plays an important role in society, it becomes the primary source to the Internet for most of the population. The deployment of 4G LTE technology makes the data accessibility fast and still evolving. ZUC is a stream cipher based security algorithm designed by Data Assurance and Communication Security Research Center (DACAS) at Chinese Academy of Sciences. It is used in the confidentiality and integrity algorithm 128-EEA3 and 128-EIA3 [1] of 3GPP standard as their core component for 4G. LTE is the dominant over the air interface technology across the world.

LTE security [12] involves authentication, confidentiality, hardware security and network security, however this report is mostly focused on software related security. The cryptographic algorithms used to secure the air interface and perform subscriber authentication functions were not publicly disclosed for the 2G GSM systems. The GSM makes uses of A3, A5, and A8 algorithm, A5 provides confidentiality, and A3 and A8 is for authentication. The UEA and UIA algorithms are used within UMTS for security. A 128-bit block cipher called KASUMI UEA1 is used for 3G security. UIA1 is a message authentication code based on KASUMI. UEA2 is a stream cipher related to SNOW 3G, and UIA2 computes a MAC using SNOW for authentication. In mobile communication networks, authentication refers to the process of determining whether a user is an authorized subscriber to the network that he/she is trying to access. Among various authentication procedures available in such networks, EPS AKA (Authentication and Key Agreement) procedure is used in LTE networks for mutual authentication between users and networks. The EPS AKA procedure consists of two steps.

1. First, an HSS (Home Subscriber Server) generates EPS authentication vector(s) (RAND, AUTN, XRES, K*ASME*) and delivers them to an MME.
2. Then in the second step, the MME selects one of the authentication vectors and uses it for mutual authentication with a UE and shares the same authentication key (K*ASME*) each other. Mutual authentication is the process in which a network and a user authenticate each other.

In LTE networks, since the ID of the user's serving network is required when generating authentication vectors, authentication of the network by the user is performed in addition to authentication of the user by the network.

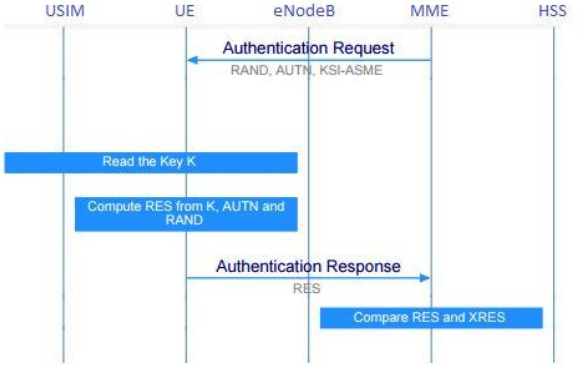

Fig. 1 LTE Authentication[1]

LTE introduced a new set of cryptographic algorithms, there are 3 sets of algorithms for both confidentiality and integrity. They are known as EPS Encryption Algorithms (EEA) and EPS Integrity Algorithms (EIA). EEA1 and EIA1 are based on SNOW 3G, EEA2 and EIA2 are based on the Advanced Encryption Standard (AES) with EEA2 defined by AES in CTR mode and EIA2 defined by AES ciphered MAC. EEA3 and EIA3 are both based on a Chinese cipher ZUC. The detailed introduction to ZUC and its descendants is in the next section.

II. ZUC ALGORITHM

ZUC, the word-oriented stream cipher, is the basic building block for both 128-EEA3 and 128-EIA3 [1] [2]. It is composed of three components with an internal state of 560 bits initialized by a 128-bit cipher key K and a 128-bit initialization vector IV, and outputs a keystream of 32-bit words. This keystream can be used to encrypt the plaintext. ZUC works in two stages initialization mode and working mode divided into three logical layers, as listed below [3].

1. Linear feedback shift register (LFSR): The LFSR is constructed from 16 register units, each holding 31 bits, and the feedback is defined by a primitive polynomial over the finite field GF(2^{31}-1). The LFSR has 2 modes of operations: the initialization mode and the working mode:
   (a) Initialization mode LFSR: the LFSR receives a 31- bit input word u,which is obtained by removing the rightmost bit from the XOR of the 32-bit output W of the F. Given below is the algorithm for initialization mode of LFSR.

   Algorithm 1 LFSR Initialization Mode:

   1: $v := 2^{15}S_{15} + 2^{17} S_{13} + 2^{21}S_{10} + 2^{20} S_4 + 28 S_0 + S_0 \bmod (2^{31} \quad 1)$
   2: u=W ⊞1
   3: $S_{16} := (v + u) \bmod (2^{31} \quad 1)$
   4: if $S_{16} = 0$ then
   5: $S_{16} = 2^{31} - 1$
   6: $(S_1, S_2, \ldots, S_{15}, S_{16}) \; ! \; (S_0, S_1, \ldots, S_{14}, S_{15})$

   (b) Working mode LFSR: produces actual keystream bits.

   Algorithm 2 LFSR Working Mode

   1: $S_{16} = 2^{15} S_{15} + 2^{17} S_{13} + 2^{21} S_{10} + 2^{20} S_4 + 28 S_0 + S_0 \bmod (2^{31} - 1)$
   2: if $S_{16} = 0$ then
   3: $S_{16=} \; 2^{31} \quad 1$
   4: $(S_1, S_2, ..., S_{15}, S_{16}) \; ! \; (S_0, S_1, \ldots, S_{14}, S_{15})$

2. Bit-reorganization:The bit reorganization extracts 128 bits from the states of the LFSR and forms four 32-bit words, where the first three words will be used by the nonlinear function F in the bottom layer, and the last word will be involved in producing the keystream. It forms 4 of 32-bit words X_0, X_1, X_2, X_3 from the following 8 LFSR registers S_0, S_2, S_5, S_7, S_9, S_{11}, S_{14}, S_{15}, as illustrated in "Fig. 2".[4]

   Algorithm 3 Bit Reorganization

   1: $X_0=S_{15H} \| \; S_{14L}$
   2: $X_1=S_{11L} \| \; S_{9H}$
   3: $X_2=S_{7L} \| \; S_{5H}$
   4:, $X3=S_{2L} \| \; S_{0H}$

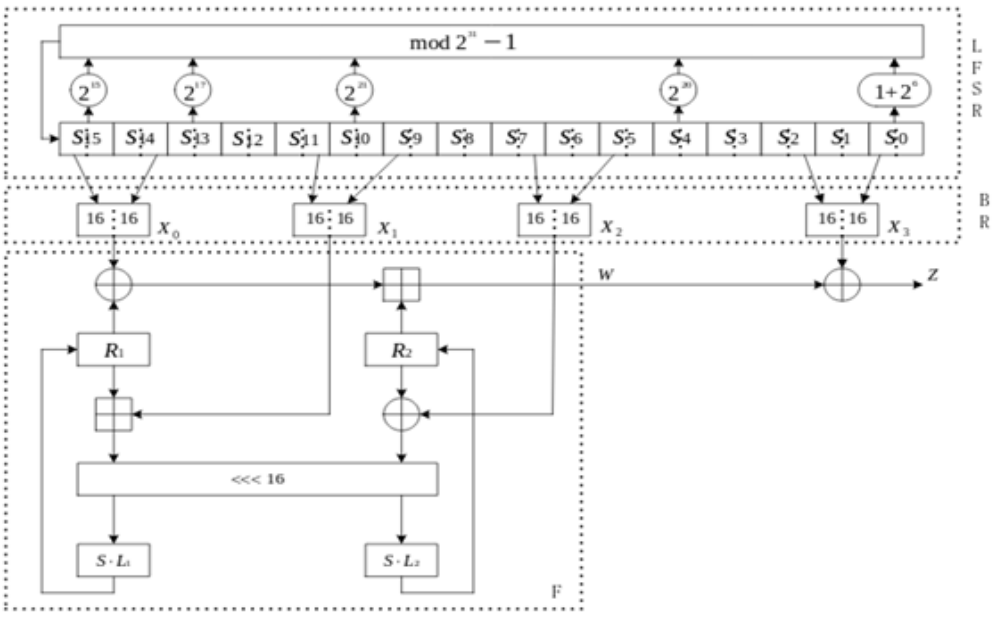

Fig. 2 Layers of ZUC [2]

3. Nonlinear function:The nonlinear function F has two 32-bit memory cells R1 and R2. Let the inputs to F be X0, X1 and X2, which come from the outputs of the bit-reorganization. Then function F outputs a 32-bit word W [3].
   The 32 x 32 S-box S is composed of four 8 8 mini S boxes, 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. L_1 and L_2 are linear transformations from 32-bit words to 32-bit words
   Algorithm 4 Nonlinear Function
   1: $W = (X_0 \quad R_1) + R_2 \bmod 2^{32}$;
   2: $W_1 = R_1 \quad X_1$;
   3: $W_2 = R_2 \quad X_2$;
   4: $R_1 = S(L_1(W_{1L} \| W_{2H}))$;
   5: $R_2 = S(L_2(W_{2L} \| W_{1H}))$;
4. Key Loading: The main part of the ZUC execution is initialization of key, how the key is loaded into the LFSR. The key initialization expands the 128 bit key and 128 bit IV to form the LFSRs initial state.
   $$K = k_0 \| k_1 \| \ldots \| k_{15}$$
   and
   $$IV = iv_0 \| iv_1 \| \ldots \| iv_{15}$$
   Along with K and IV, a 240 bit constant D is used in key loading. Each ofthe LFSR bits S1 to S15 is calculated as
   $$s_i = k_i \| d_i \| iv_i, \text{ for } i = 0, 1, \ldots, 15$$
5. ZUC Execution:
   (a) Initialization phase: All the steps are performed for 32 cycles to load the key into LFSR. Given below is the quick overview of Initialization phase of ZUC algorithm.
   for (i=0 to 31){
   Bit Reorganization
   Nonlinear Function Calculation
   LFSR Initialization Mode
   }
   (b) Working Phase Keystream mode is similar to initialization, but the LFSR does not receive any input. The output *W* of non-linear function is xored with X3 (word extracted on bit reorganization layer)producing keystream word Z. The output word W produced by nonlinear function is discarded is discarded for first clock and then thekeystream is calculated as
   $Z = W \oplus X3$;

III. CRYPTANALYTIC ATTACKS

A. Time-Memory-Data Trade-Off Attacks[8]*:*

The ZUC algorithm takes 128-bit secret key, 32-bit COUNT, 5-bit BEARER and 1-bit DIRECTION as input. These input together forms an non-secret Ini-tialization Vector (IV) for the encryption. The 5-bit BEARER is unpredictable by an attacker intercepting encrypted messages – the COUNT is reset to 0 for each new secret key, and DIRECTION is uplink or downlink. The key points noticed for TMTO attacks are:

1. Babbage-Golic tradeoff:
   Compute and store a table of 2^m key-IV pairs and the keystreams, the attacker can probably determine the key and used to generate one of the intercepted keystreams. The table can be computed once, and then used for repeated attack attempts on different sets of intercepted keystreams.
2. Biryukov-Shamir tradeoff: By precomputing 2^p key/IV pairs, and storing a table of size 2^m, an attack is possible with online time complexity t as long as t 2d, p+d k+v, and m+t k+v. For example, with 2^{40} keystreams, an attack is possible with oneoff precomputation time 2^{93}, and online time complexity 2^{80}, but computer memory requirement only 2^{53}.
   Also they state that if the number of unpredictable IV bits are increased, the complexity of these attacks also increases.

B. Chosen IV Attacks[12]*:*

These attacks target at the initialization stage of stream ciphers. The Key-IV bits are used to generate a complex internal states, thus any difference in the Key-IV may result in unpredictable internal state and produce different output keystreams. The ZUC initialization process has 32 iterations. The changes in the internal states are studied for every iteration of a specific Key-IV pair. After some analysis, the attackers have made some assumptions:

1. ΔIV[3], 0 and the remaining 15 bytes of ΔIV are all 0, The outcomes identifies that the differences in LFSR and the memory cells *R*1 and *R*2 propagate very slowly. Here ΔIV is the difference of IV's.
   Considering ΔIV[3]=*a*, and other bits as 0, the differences of the 16 cells of the LFSR before the 1*st* round iteration are:
   $$(S0, S2, S5, S7, S9, S11, S14, S15) = (0,0,0,0,0,0,0,0,0,0,0,0,a,0,0,0)$$
   As initialization process takes 32 round iterations, the s0=0 after 18 rounds, which means that the LFSR state is not random even after 18 rounds ofiterations. Also the difference variation of *R*1 and *R*2 is zero after 7 iterations. Even after the 8-th round of iteration, the difference of *R*1=0 and *R*2≠0. The differences of *R*1 and *R*2

have better randomness with the in-crease of the number of rounds of iteration. Thus from this behavior it is believed that, after 32 rounds of iteration, the differences of $R1$ and $R2$ will be fairly random and unpredictable.

2. Key[8] , 0 and the remaining 15 bytes of Key are all 0,
   The outcomes identifies that difference in LFSR propagates slowest. We have that $s0=0$ after 19 rounds.

C. Guess-and-Determine Attack[5]*:*

These attacks works by guessing part of internal states of the target algorithm,combining with some known mathematical relations for the algorithm, to deduce the remaining unknown internal states. ZUC appears to have strong resistance against guess-and-determine attacks. It is seen that the ZUC algorithm has 16×31+2×32=560 bits of internal states. If an attacker tries to find internal states at some time interval, and tries to guess r bits of these states to determine the remaining 560-r states. Then the attacker needs at least (560-r)/32 key-words to establish algebraic equations, to determine the remaining unknown bits.

For a successful guess-and-determine attack r<128.

If the attacker tries to guess the values of the memory cells R1 and R2 in different time intervals, then the number of bits to be guessed is apparently no less than 128.

D. Weak key Attacks[10]*:*

There is a one-to-one mapping from the initial state of ZUC to the state after its initialization. So suppose that the state $(s_0,s_1,\ldots,s_{15},R_1,R_2)$ clocks to$(s'_0,s'_1,\ldots,s'_{15},R'_1,R'_2)$ and that X_0, X_1 and X_2 are the words derived from the former state. Given $(s'_0,s'_1,\ldots,s'_{15},R'_1,R'_2)$, one can:

1. Compute $s_1,s_2,\ldots,s_{15}$ from $s'_0,s'_1,\ldots,s'_{14}$
2. Compute X_0, X_1 and X_2 from $s_1,s_2,\ldots,s_{15}$
3. Compute R_1 and R_2 from R'_1,R'_2, X_1 and X_2
4. Compute the output W of the nonlinear function F from X_0, R_1 and R_2
5. Compute s_0 from s_1, $s_2,\ldots,s_{15},s'_{15}$ and W:

$s'_{15} = 2^{15}s_{15}+2^{17}s_{13}+2^{21}s_{10}+2^{20}s_4+257s_0+(w>>1) \bmod (2^{31}-1)$

If all cells of s_i are equal to p after the ZUC initialization with K and IV, the corresponding key K is called a weak key.

E. SAT based Attacks[7]*:*

The satisfiability is a decision problem, given a propositional formula such that assigning value to the equation satisfies the result. The application to cryptanalysis is straightforward: informally, if a formula f(k,x,y) encodes an encryption y = Ek(x), then an adversary can plug into f(k,x,y) known values for x,y and obtain a simpler formula f0(k) which can be fed to a SAT solver in order to recover the key k. The package cryptosat allows to quickly verify someissues with ZUC that were left open in previous works. The cryptosat packagehelps to see under which condition weak states can be reached. It generatesSAT instances encoding the Key-IV initialization. The SAT solver returns theweak input if satisfied otherwise it do not return anything. They found thatno weak inputs exists when R1=R2=0. As soon as R1 or R2 can be chosen,weak states can be reached for reduced round versions, although the numberof satisfiable instances decreases as a function of the number of rounds. Theseweak state have no concern to the security feature of ZUC [6][7].

F. Power Analysis of ZUC [10]:

ChunfangZhou et al. extend the differentialpropertiesof the initialization stage of ZUC algorithmfrom 20 roundsto four more rounds and shows that ZUC can still resist against chosen-IV attacks [19]. However, whether ZUC can resist against DPA is rather unknown.Their analysis results shows ZUC is vulnerable to DPA.

1. Collection of power consumption data.
2. The value of R1 and R2 registers and the state of the 16 LFSR derived in the round one are used in the next round for initialization.
3. Determination of key information for different rounds separately.
4. Performthe DPA in the sixth round of the initialization stage to make an exhaustive search.
5. Determine the unknown byte of the secret key.

The core idea of this strategy is to use a configurable switch matrix to control the position of registers in between functional blocks of an algorithm [10].

IV. CONCLUSION AND FUTURE WORK

In this paper a detailed review of ZUC stream cipher for security of LTE algorithm is discussed. Also how the keystream is generated for encryption. This algorithm is used in third set of EEA and EIA for confidentiality and integrity. Some attacks were also described in the last section which are used for analysis of ZUC. In future these attacks could be combined to improve the complexity and recover the key from the data available. From the assumed keystream from which algebraic expressions could be built which can then be solved using SAT solver by combining algebraic attacks with SAT based attacks.

REFERENCES

[1] 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.
[2] ETSI/SAGE Specification. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification; Version: 1.6.
[3] ETSI/SAGE Technical report, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 4: Design and Evaluation Report, Version: 2.0.
[4] ALMashrafi MJ. A different algebraic analysis of the zuc stream cipher. In: Proceedings of the 4th International Conference on Security of Information and Networks, SIN '11. New York, NY, USA: ACM; 2011.
[5] Lin D, Shu-kai L, Zhong-ya Z, Jie G. Guess and determine attack onzuc based on solving nonlinear equations. In: First International Workshop on ZUC Algorithm; 2010.
[6] Frédéric Lafitte , Olivier Markowitch , Dirk Van Heule, SAT based analysis of LTE stream cipher ZUC, Proceedings of the 6th International Conference on Security of Information and Networks, p.110-116, November 26-28, 2013.
[7] Lafitte F. cryptosat: An extensible package for SAT-based cryptanalysis, r package version 0.1.0. 2014.
[8] Biryukov A, Shamir A. Cryptanalytic time/memory/data tradeoffs for stream ciphers. In: Okamoto T, editor. Advances in cryptologyeASIACRYPT. Lecture notes in computer science, Vol. 1976. Springer; 2000.
[9] Ghizlanem Orhanou and Said El-Hajji, "The New LTE Cryptographic Algorithms EEA3 and EIA3," in International Journal of Applied Mathematics & Information Sciences, vol. 7, no. 6, pp. 2385-2390, 2013.
[10] P.C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In Advances in Cryptology – CRYPTO 1999, volume 1666 of Lecture Notes in Computer Science (LNCS), pages 388–397. Springer, 1999
[11] L. Ji, Improved differential paths of zuc, in: 1st International Workshop on ZUC Algorithm, 2010.
[12] Yan Ying-jian. Chosen-IV Correlation Power Analysis Attack of ZUC Stream Cipher, Journal of Electronics & Information Technology, 2015
[13] Michael Bartock, LTE Security – How Good Is It?, National Institute of Standards & Technology, US Department of Commerce.

BIOGRAPHY

Saurabh Lawange is a student in the Information Technology Department, Walchand College of Engineering, Sangli, India. Heis pursuinghis Master's degree from WCE, Sangli, MS, India. His research interests are Computer Networks, Information Security, Databases, Bigdata etc.

Manish Narnaware is assistant professor in the Information Technology Department, Walchand College of Engineering, Sangli, India. His research interests are Computer Networks, Information Security, Image Processing etc.

