International Journal of Engineering & Technology, 7 (4.15) (2018) 519-523

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Analysis the Components of SNOW 3G and ZUC Ciphers in Mobile Systems

Khalid Fadhil Jasim[1]*, Imad Fakhri Al-Shaikhli[2]

[1]*Department of Computer Science, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia*
[2]*IIUM Cyber Security Malaysia Center for Cyber Space Security Kuala Lumpur, Malaysia*
**Corresponding author E-mail: khalid.jassim@yahoo.com*

Abstract

The SNOW 3G and ZUC ciphers algorithms are classified as stream ciphers, used as confidentiality algorithms in third and fourth generations of Mobile Technologies (3G-UMTS and 4G- LTE). This research, focused on analyzing and evaluating randomness properties of various components of SNOW 3G and ZUC stream ciphers. Software programs of these ciphers and NIST (SP 800-22) tests adopted to assess the randomness properties. Many experiments conducted on output sequences of SNOW 3G and ZUC ciphers components. Practical experiments results confirmed that all SNOW 3G main components passed NIST tests. However, some components of ZUC Cipher passed NIST randomness tests, while significant components failed in NIST tests. Weaknesses pinpointed in randomness properties of ZUC cipher may be exploited by statistical cryptanalysis attacks, due to certain patterns appeared in the output sequences of failed ZUC Cipher components.

Keywords: *SNOW 3G Cipher; ZUC Cipher; Keystream; Register LFSR; Bit Reorganization; S-box; Randomness Tests.*

1. Introduction

The third generation (3G-Mobile systems) appeared in (2000s) and presented various standards like Universal Mobile Telecommunication Systems (UMTS). Mobile 3G relied on mobile broadband technologies and supported some services for the mobile customers such as (Multimedia Applications, High speed Internet services, Voice Calls with digital technology and Video Conferencing on Mobile Net.). Also, 3G-Systems offered enhanced features (e.g., increased the capacity of voice and data transmissions, packet data transmissions over Mobile Networks and provided Mobile Services with high speed data transmissions). For instance, 3G-Systems with (HSPA and WCDMA standards) offered transmissions data rates (14.4 Mbps and reached up to 63+ Mbps). The CDMA2000 and EV-DO standards supported transmissions rates (e.g. from 3.1 Mbps and up to 14.7 Mbps) [1].

Moreover, the Mobile technology of fourth generation (4G-Mobile systems) introduced in (2010s). 4G-systems presented some standards such as LTE-technology, which is the Long-Term Evolution, and supported a fast broadband technology. Many mobile services offered by 4G-LTE like (Cloud computing, HD Mobile TVs, Mobile Web Access and Services of IP Telephony). Also, this technology offered data rate transmissions of (50 Mbps) for uplink and with (100 – 326.4 Mbps) in case of down link data transmissions. Multiple antenna adopted in (4G-LTE), in which improved data and voice capacity, efficiency, and rate of data transmissions in these systems [2].

Symmetric cryptographic algorithms proposed to support information confidentiality and information integrity in different mobile generations. These algorithms relied on Block Ciphers and Stream Ciphers techniques. In this context, SNOW 3G Cipher designed based on stream ciphers techniques. SNOW 3G was adopted as confidentiality algorithm (UEA2) and used to encrypt the data in 3G systems (3G-UMTS). Structure of SNOW 3G includes some components, LFSR register, nonlinear part which is the finite state machine (FSM) and three memory registers R1, R2 and R3 [3].

Various cryptanalysis methods used on SNOW 3G Cipher. For example, Differential cryptanalysis attack applied on SNOW 3G. This analysis method focused on initialization operation stages from Clock number (1) to Clock number (32) of the cipher initialization. Also, this method can proceed when there is no data feedback between FSM and LFSR register during initialization stage. The cryptanalyst of SNOW 3G, in differential attack with known IV key, requires information of pairs of IV keys values (e.g. In practical, IV key values transmitted via open mobile communications, so it can be captured by intruders). The complexities of Differential attack method included data complexity (233 of output keystream) and time complexity of (257) [4].

The ZUC Cipher used for information security in 4G-LTE mobile technology systems. For information confidentiality, the confidentiality cipher algorithm (128-EEA3) adopted and this algorithm was based on ZUC Cipher with secret confidentiality key (CK). On the other hand, information integrity achieved by using integrity cipher algorithm (128-EIA3) with secret integrity key (IK). The 128-EIA3 algorithm depended on ZUC Cipher [5].

In addition, the design of ZUC Cipher relied on stream cipher techniques and included basic components (e.g. Shift register LFSR, Function (F) with nonlinear properties and BR for bit reorganization). During initialization operations, secret key (K, with 128 bits) and non-secret key (IV, with 128 bits) used in this cipher. In the phase of keystream (Z) generation, sequence of words produced by ZUC Cipher, in which these words compose the Z key stream. Later, the sequence of (Z) keystream utilized in the phase of Encryption/Decryption to secure uplink and downlink data transmissions [6].

Different analysis researches conducted on ZUC Cipher. For instance, the authors of [7] analyzed space and time complexities of operations in ZUC Cipher algorithm. They pointed out linear space complexities and linear time complexities in confidentiality and integrity algorithms. Also, Differential Cryptanalysis Attacks can be used in analyzing ZUC Cipher. In this attack, certain bytes in IV key were targeted and identical values in keystream (Z) can be located. Then, these identical values may be adopted to find the actual values of secret key (K) based on searching technique with complexity value (299.4) [8].

The randomness of output sequence for various components of cipher algorithms effects on the security of these ciphers. For instance, different tests can be used to check the security of stream cipher algorithms, the authors in [9] proposed the statistical tests (Run test, Frequency test, Correlation test and execution time) to assess the security of stream cipher algorithms used in Mobile LTE network, and they focused on randomness of the generated keystream.

Also, the randomness confirms that output sequence must be unpredictable, independent, and uniformly distributed [10]. This research concentrated on analyzing the randomness of various components of SNOW 3G and ZUC Ciphers. Statistical Test Suit (NIST-SP 800-22) [11] has been adopted to analyze and assess different components of SNOW 3G and ZUC Ciphers.

This research organized as follows. Various components of SNOW 3G Cipher, initialization and keystream operation phase are described in section 2. The components of ZUC Cipher, initialization operation and keystream generation mode are showed in section 3. In section 4, evaluation of randomness properties of SNOW 3G and ZUC Ciphers are conducted. Section 5 discussed the experimental results. Section 6 concluded the research results.

2. Discription of Snow 3G Cipher

The SNOW 3G Cipher classified as stream cipher, proposed by (ETSI/SAGE) and used in 3rd generation (3G-UMTS) Mobile systems for information confidentiality algorithm. Initialization of SNOW 3G relies on secret key K (K, consists of 128 bits) and Initial key Vector (IV, consists of 128 bits). The structure of SNOW 3G includes Register LFSR (LFSR contains sixteen words (32-bit), S0, S1, S2, S3 … , and S15) and Non Linear Function (FSM, which is the finite state machine). FSM consists of memory registers (R1, R2 and R3 with 32-bit for each of them), and Substitution Boxes (i.e. S-Box S1 & S-Box S2, which relied on input of 32-bit and output with 32-bit) (Figure 1) [12].

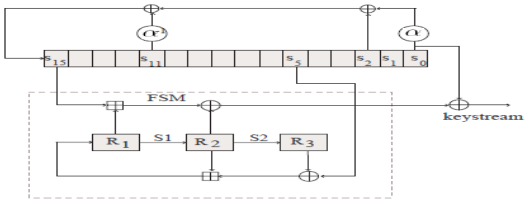

Fig. 1: Snow 3G Cipher [12]

SNOW 3G can work in keystream operation phase (Figure 1). The kestream phase is shown in the following three Steps. First, clock the components of Finite State Machine (FSM, as shown in Step #1 below) and compose output F (F, consists of 32-bit word), calculation of word F relies on (32-bit word S15 from LFSR, 32-bit word of register R1 and 32-bit word of register R2). Second, compute 32-bit word of keystream (ZI , as in Step #2) which depends on (word F from FSM and word S0 extracted from register LFSR). Finally, update the contents of register LFSR according to feedback function of Word V and shift the 16 words (S0, S1, S2, S3, and S15) of LFSR as described in Step #3 below [13].

For I = 1 to N (N represents number of generated 32-bit words of keystream)

{ Step #1: Clock Components of FSM, Calculate output F (F is 32-bit word):
Output F = ((S15 ⊞ R1) **XOR** R2), (Math operation ⊞ is addition mod 232)
Word r = (R2 ⊞ (R3 **XOR** S5)), word S5 extracted from LFSR.
Register R3 = Sub-Box-S2 [R2],
Register R2 = Sub-Box-S1[R1], and
Register R1 = Word r.
Step #2: Compute Keystream ZI, represent output keystream word (32-bit):
Keystream ZI = (F **XOR** S0), word S0 extracted from LFSR.
Step #3: Shift all stages of LFSR register:
Word V = (S0,1 || S0,2 || S0,3 || 0x00) **XOR MULα**(S0,0) S2 **XOR** (0x00 || S11,0 || S11,1 || S11,2) **XOR DIVα** (S11,3).
Shift 16 words of LFSR:
Word S0 = S1, Word S1 = S2, Word S13 = S14,
Word S14 = S15, and Word S15 = Word V.}

3. Description of ZUC Cipher

The design of ZUC Cipher classified as stream cipher and consists of three basic parts (Part 1: Shift Register LFSR, Part 2: Bit-Reorganization BR and Part 3: Nonlinear Function F). In part 1, Shift Register LFSR includes sixteen-stages (S0[31-bit], S1[31-bit], …, S15[31-bit]). Also, LFSR is operated in 2 phases (Phase#1: Initialization Mod and Phase#2: Working Mod). In Phase#1, the 32-bit word W is taken as output from function F, then the word u is computed based on shifting word W to right direction with one bit. The word V is calculated, as feedback function of register LFSR, by adding with Mod (231-1) the LFSR words (S15, S13, S10, S4, and S0). The LFSR word (S16) is computed by adding with Mod (231-1) the words (u and V). Then updating the contents of LFSR words (i.e. S0 = S1, S1 = S2, S15 = S16). In Phase#2, the word (S16) is computed by adding Mod (231-1) the LFSR words (S15, S13, S10, S4, and S0). Then the contents of LFSR words will be updated as mentioned before. In the aforementioned Phases, if the word (S16) contains zero values then it will be set to vale (231-1) [14].

Phase#1:LFSR in Initialization Operation Mode

{W is 32-bit word selected as output from nonlinear function F.
u = W >> 1 (1-bit right shift of W)
$V = (2^{15}S_{15} + 2^{17}S_{13} + 2^{21}S_{10} + 2^{20}S_4 + (1+2^8)S_0) \bmod (2^{31}-1)$;
$S_{16} = (V + u) \bmod (2^{31}-1)$;
If $S_{16} = 0$, the $S_{16} = 2^{31}-1$;
$(S_0, S_1, \ldots S_{14}, S_{15}) \leftarrow (S_1, S_2, \ldots S_{15}, S_{16})$}

Phase#1: LFSR in Initialization Operation Mode

{$S_{16} = (2^{15}S_{15} + 2^{17}S_{13} + 2^{21}S_{10} + 2^{20}S_4 + (1+2^8)S_0) \bmod (2^{31}-1)$;
$(S_0, S_1, .S_{14}, S_{15}) \leftarrow (S_1, S_2, .S_{15}, S_{16})$}

In Part 2 (Bit-Reorganization, BR), eight elements of register LFSR (Stages: S0, S2, S5, S7, S9, S11, S14, S15) are extracted to compose (128 bits). Also, the composed (128 bits) are adopted to create 4 (32-bits) words denoted by (X0, X1, X2, X3). Then, the 32-bit words (X0, X1, X2) are used to compute function F (i.e. input to F, F(X0, X1, X2). However, the word (X3) is XORD with the output of function F and to compose the word (32-bit) of Z keystream.

Bit Reorganization BR( )
{X0 = $S_{15}H \| S_{14}L$; (where H is leftmost (16 bits) of word S_{15}, and‖is concatenation)
X1 = $S_{11}L \| S_9H$;
X2 = $S_7L \| S_5H$;

$X3 = S_2L \| S_0H.\}$

In Part 3 (Function F), the internal structure of function F consists of 2 (32-bit) Registers (R1, R2), Substitution Box (S-Box with (32 x 32 Bits)). The computation of function F relies on input of words (X0, X1, X2), 32-bit words W1 and W2, 32-bit registers R1 and R2, and using S-Box. Then, the output of this function will be stored in 32-bit word (W).

Nonlinear Function F(X0, X1, X2)
{W = (X0 ⊕ R1)⊕R2; (⊕ is exclusive OR, ⊕ is addition mod 2^{32})
W1 = R1 ⊕ X1;
W2 = R1 ⊕X2;
R1 = S-Box S(L1 (W1L ‖ W2H); (where L is rightmost (16 bits) of word W1)
R2 = S-Box S(L2 (W2L ‖ W2H). (where H is leftmost (16 bits) of word W1)}

Also, L1 and L2 are linear transformations used during internal calculations of function F.

$L1(X) = X \oplus (X <<< 2) \oplus (X <<< 10) \oplus (X <<< 18) \oplus (X <<< 28)$,
$L2(X) = X \oplus (X <<< 8) \oplus (X <<< 14) \oplus (X <<< 22) \oplus (X <<< 30)$.
Where X <<< n, is the n-bit cyclic shift of 32-bit word X to the left).

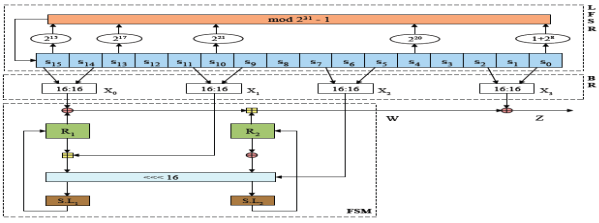

Fig. 2: ZUC Cipher [15]

In addition, the keystream (Z) is calculated during the ZUC cipher working in keystream operation mod. The 32-bit word of keystream (Z) at time (t) is computed based on words (X0, X3, registers R1 and R2) [16].

$$Z^t = ((X_0^t \oplus R_1^t) + R_2^t) \oplus X_3^t \quad (1)$$

4. Randomness Properties of Snow 3G and ZUC Ciphers

The Block ciphers and stream ciphers are based on different components (e.g. Nonlinear Functions, Memory Registers, LFSR Registers, Substitution Boxes, Permutation Tables, etc …). These components produce output data of keystreams and sequences. In light of data security, these output data must possess randomness properties (i.e. unpredictable, independent, and uniformly distributed)[17, 18]. These randomness properties will enhance the security of block and stream ciphers, in which can withstand against some statistical cryptanalysis attacks. Thus, this research focuses on NIST test (SP 800-22) [19] to assess randomness properties of various components for SNOW 3G and ZUC ciphers.
The NIST (SP 800-22) suit relies on some tests to evaluate the randomness and as shown in (Tables 2 to 6). In NIST suit, each test calculates value of p (called p-value). The p-value must be compared with defined significance level (α, where α = 0.01 in our experiments). If the p-value (p ≥ α), then the produced data (keystreams or sequences) possess random behavior. On the other hand, if p-value (p < α), then the produced data is not random[20].
Moreover, NIST test adopted to assess the randomness of different components of SNOW 3G and ZUC ciphers. In this context, simulation software programs of SNOW 3G and ZUC ciphers, used to compose data of outputs with sample (Size, S =100), length of each sample (n=220 , or n= one Mega Bit). During practical experiments on simulation programs, random values used for secret K (128-bits) and initialization key IV (128-bits). Also, in practical experiments the parameters of NIST test are defined as in Table 1.

Table 1: Defined Parameters for NIST Tests

Randomness Tests and Other Parameters	Input Parameter values (In bits)
Block factory test (Block Length)	M=128
Non-overlapping template test (Block length)	m=9
Overlapping template test (Block length)	m=9
Approximate entropy test (Block length)	m=10
Series Test (Block Length)	m=16
Linear complexity test (Block length)	M=500
Sequence Length	$N=2^{20}$
Sample size or no of sequences	S=100
Significance level α	α=0.01

5. Discussion of Experimental Results

The NIST tests performed on different components of SNOW 3G and ZUC ciphers such as (Keystream, F Function, S-Boxes, Registers R1, R2, LFSR and Bit Reorganization). Simulation software programs of SNOW 3G and ZUC Ciphers were used to compose (100) output sequences for each of these components. Practical results have been analyzed as follows:

- In SNOW 3G Ciphers, Randomness results of (Keystream, FSM, S-box S1, and S-box S2) are shown in (Table 2). For instance, in case of output keystream , the minimum p-value was (0.051942, in the Universal test), the maximum p-value was (0.978072, in Cumulative Sums (Forward) test). Also, it was noticed all the p-values of the mentioned components, were greater than α (α = 0.01). Thus, SNOW 3G components (Keystream, FSM, S-box S1, and S-box S2) were passed NIST randomness tests.
- Randomness results of (Registers R1, R2, R3 and LFSR) are depicted in (Table 3). For example, in case of output for register R1, the minimum p-value was (0.304126, in Cumulative Sums (Forward) test), the maximum p-value was (0.971699, reported in FFT test). Moreover, the p-values of these registers were greater than α (α = 0.01). Therefore, SNOW 3G registers R1, R2, R3 and LFSR were passed randomness tests.
- In ZUC cipher, Table 4 shows Randomness results of (Keystream, F Function, S-Box S0 and S1). For instance, in keystream, the minimum p-value was (0.058984, in frequency test), the maximum p-value was (0.883171, in linear complexity test). Furthermore, the p-values of these components were greater than α (α = 0.01), in which indicates ZUC components (Keystream, F Function, S-Box S0 and S1) were passed randomness tests.
- Practical results of (Registers R1, R2 and LFSR) are described in (Table 5). For the output of register R2, the minimum p-value was (0.028817, in FFT test), the maximum p-value was (0.924076, reported in Block Frequency test). Moreover, the p-values of registers R1 and R2 were greater than α (α = 0.01), which means that R1 and R2 passed randomness tests. On the other hand, register LFSR was failed in 15 NIST randomness tests, due to the p-values of these tests were (0.0, i.e. p-values less than α, and α = 0.01) (Table 5).`
- Results of other ZUC components (i.e. Bit Reorganization BRCX0, BRCX1, BRCX2 and BRCX3) are shown in (Table 6). In BRCX0, the minimum p-value was (0.0, in Block Frequency test), which indicates that BRCX0 was failed in Block Frequency. Also, due to the p-values were (0.0) in some tests, it was clear that BRCX1 failed in FFT and Block Frequency tests. BRCX2 was failed in Random Excursions

and Block Frequency tests. BRCX3 was failed in Block Frequency test.

As results, in case of SNOW 3 G Cipher, all basic components (i.e. Keystream, FSM, Substitution Boxes, Registers R1, R2, R3 and LFSR) were passed NIST randomness tests. For ZUC Cipher, some weaknesses were found in randomness properties of some components (i.e. Bit Reorganization(BRCX0, BRCX1, BRCX2 and BRCX3), and Register LFSR). These weaknesses in randomness are undesirable and lead to appear some patterns in output sequences of the failed components. Also, the appearance of weak patterns may be exploited via statistical cryptanalysis attacks against ZUC cipher based on divide and conquer scenario.

Table 2: Randomness Results of Keystream, FSM, S-box S1, and S-box S2 for SNOW 3G**.**

Test No.	Statistical Test	P-Value of Keystream	P-Value of FSM	P-Value of S-box S1	P-Value of S-box S2
1	Frequency	0.657933	0.657933	0.171867	0.867692
2	Block-Frequency	0.289667	0.419021	0.319084	0.514124
3	Cumulative Sums(Forward)	0.978072	0.171867	0.798739	0.851383
	Cumulative Sums(Reverse)	0.137282	0.867692	0.289667	0.798139
4	Runs	0.851383	0.090936	0.999438	0.834308
5	Longest Run	0.719747	0.319084	0.798139	0.058984
6	Rank	0.304126	0.739918	0.759756	0.779188
7	FFT	0.319084	0.085587	0.080519	0.401199
8	Non-Overlapping Template	0.851383	0.574903	0.798139	0.419021
9	Overlapping Template	0.474986	0.616305	0.616305	0.181557
10	Universal	0.051942	0.719747	0.883171	0.289667
11	Approximate Entropy	0.236810	0.350485	0.494392	0.249284
12	Random Excursions	0.756476	0.141256	0.224821	0.517442
13	Random Excursion Variant	0.155209	0.788728	0.719747	0.337162
14	Serial 1	0.437274	0.085587	0.304126	0.996335
	Serial 2	0.437274	0.637119	0.171867	0.987896
15	Linear Complexity	0.383827	0.181557	0.153763	0.275709

Table 3: Randomness Results of Registers R1, R2, R3, and LFSR for SNOW 3G.

Test No.	Statistical Test	P-Value of Register R1	P-Value of Register R2	P-Value of Register R3	P-Value of Register LFSR
1	Frequency	0.574903	0.864692	0.911413	0.739918
2	Block-Frequency	0.699313	0.699313	0.514124	0.474986
3	Cumulative Sums(Forward)	0.304126	0.595549	0.213309	0.171867
	Cumulative Sums(Reverse)	0.419021	0.867692	0.262249	0.455937
4	Runs	0.759756	0.401199	0.213309	0.383827
5	Longest Run	0.334538	0.437274	0.236810	0.350485
6	Rank	0.779188	0.816537	0.574903	0.595549
7	FFT	0.971699	0.028817	0.595549	0.637119
8	Non-Overlapping Template	0.616305	0.554420	0.637119	0.616305
9	Overlapping Template	0.897763	0.678686	0.851383	0.334538
10	Universal	0.867692	0.129620	0.955835	0.719747
11	Approximate Entropy	0.419021	0.319084	0.574903	0.015598
12	Random Excursions	0.378183	0.141256	0.275709	0.911413
13	Random Excursion Variant	0.324180	0.819544	0.437274	0.051001
	Serial 1	0.719747	0.366918	0.924076	0.102526
14	Serial 2	0.534146	0.020548	0.616305	0.071177
15	Linear Complexity	0.678686	0.05358	0.678686	0.085587

Table 4: Randomness Results of Keystream, Function F, S-box S0, and S-box S1 for ZUC.

Test No.	Statistical Test	P-Value of Register R1	P-Value of Register R2	P-Value of Register R3	P-Value of Register LFSR
1	Frequency	0.058984	0.678686	0.366918	0.699313
2	Block-Frequency	0.719747	0.249284	0.924076	0.534146
3	Cumulative Sums(Forward)	0.249284	0.334538	0.514124	0.455937
	Cumulative Sums(Reverse)	0.096578	0.895549	0.739918	0.080519
4	Runs	0.719747	0.851383	0.437274	0.678686
5	Longest Run	0.534146	0.080519	0.101199	0.4944392
6	Rank	0.798139	0.935716	0.851383	0.534146
7	FFT	0.383827	0.759756	0.657933	0.739918
8	Non-Overlapping Template	0.23681	0.304126	0.534146	0.202268
9	Overlapping Template	0.224821	0.494392	0.987896	0.935716
10	Universal	0.851383	0.637119	0.058984	0.019188
11	Approximate Entropy	0.494392	0.699313	0.851383	0.834308
12	Random Excursions	0.551026	0.289667	0.654467	0.875539
13	Random Excursion Variant	0.222869	0.23681	0.204076	0.364146
	Serial 1	0.867692	0.779188	0.55442	0.514124
14	Serial 2	0.080519	0.616305	0.739918	0.383827
15	Linear Complexity	0.883171	0.153763	0.678686	0.058984

Table 5: Randomness Results of Registers R1, R2 and LFSR for ZUC.

Test No.	Statistical Test	P-Value of Register R1	P-Value of Register R2	P-Value of Register LFSR
1	Frequency	0.437274	0.861692	0.000000
2	Block-Frequency	0.042808	0.924076	0.000000
3	Cumulative Sums(Forward)	0.971699	0.275709	0.000000
	Cumulative Sums(Reverse)	0.883171	0.455937	0.000000
4	Runs	0.55442	0.678686	0.000000
5	Longest Run	0.514124	0.122325	0.000000
6	Rank	0.455937	0.23681	0.000000
7	FFT	0.55442	0.028817	0.000000
8	Non-Overlapping Template	0.55442	0.616305	0.000000
9	Overlapping Template	0.719747	0.249284	0.000000
10	Universal	0.816537	0.181557	0.020548
11	Approximate Entropy	0.595549	0.779188	0.000000
12	Random Excursions	0.699313	0.366918	0.000000
13	Random Excursion Variant	0.494392	0.202268	0.000000
	Serial 1	0.494392	0.699313	0.000000
14	Serial 2	0.897763	0.153763	0.366918
15	Linear Complexity	0.616305	0.514124	0.009535

Table 6: Randomness Results of Bit Reorganization BRCX0, BRCX1, BRCX2, and BRCX3 for ZUC.

Test No.	Statistical Test	P-Value of BRCX0	P-Value of BRCX1	P-Value of BRCX2	P-Value of BRCX3
1	Frequency	0.514124	0.55442	0.419021	0.699313
2	Block-Frequency	0.000000	0.000000	0.000000	0.000000
3	Cumulative Sums(Forward)	0.759756	0.739918	0.996335	0.867692
	Cumulative Sums(Reverse)	0.924076	0.851383	0.474986	0.934308
4	Runs	0.383827	0.040108	0.437274	0.075719
5	Longest Run	0.759756	0.494392	0.99425	0.924076
6	Rank	0.137282	0.935716	0.12962	0.122325
7	FFT	0.062821	0.000347	0.080519	0.026948
8	Non-Overlapping Template	0.071177	0.455937	0.080519	0.026948
9	Overlapping Template	0.574903	0.080519	0.574903	0.042808
10	Universal	0.334538	0.55442	0.23681	0.637119
11	Approximate Entropy	0.085587	0.108791	0.798139	0.011791
12	Random Excursions	0.595549	0.401199	0.00699	0.637119
13	Random Excursion Variant	0.55442	0.249284	0.77276	0.334538
	Serial 1	0.102526	0.334538	0.191687	0.719747
14	Serial 2	0.514124	0.304126	0.171867	0.366918
15	Linear Complexity	0.851383	0.534146	0.162606	0.924076

6. Conclusion

This research concentrated on analyzing various components of SNOW 3G and ZUC ciphers with emphasis on randomness properties. The NIST (SP 800-22) tests used to compute and evaluate randomness properties of SNOW 3G and ZUC components. Also, simulation software programs of SNOW 3G and ZUC ciphers were used to implement the practical experiments. Different random keys (Secret Key K and Initialization Variable IV) adopted to initialize the simulation software programs and many samples of output sequences composed for SNOW 3G and ZUC components. As a result, the main SNOW 3G components (i.e. Keystream, FSM, Substitution Boxes, Registers R1, R2, R3 and LFSR) were passed NIST randomness tests. On the other hand, practical results showed that some p-values of randomness NIST tests were (0.0). These p-values < α (α = 0.01), which confirmed that some ZUC components failed in randomness tests. Therefore, Register LFSR was failed in 15 NIST tests. Bit Reorganization BRCX0 and BRCX3 were failed in NIST Block Frequency test. Bit Reorganization BRCX1 was failed in FFT and Block Frequency NIST tests. BRCX2 was failed in Random Excursions and Block Frequency NIST tests. Finally, weaknesses have been pointed out in randomness of some ZUC components, namely Register LFSR and Bit Reorganization (BRCX0, BRCX1, BRCX2 and BRCX3). Such weaknesses may be exploited through statistical cryptanalysis attacks against ZUC cipher.

Acknowledgements

This material is based upon work supported by the IIUM under Grant No. RIGS16-366-0530

References

[1] M. J. Arshad, A. Farooq, and A. Shah, “Evolution and Development Towards 4 th Generation (4G) Mobile Communication Systems,” Journal of American Science, vol. 6, no. 12, pp. 63–68, 2010.

[2] F. Rezaei, M. Hempel, and H. Sharif, “A comprehensive performance analysis of LTE and Mobile WiMAX,” 8th Int. Wirel. Commun. Mob. Comput. Conf., pp. 939–944, Aug. 2012.

[3] ETSI/SAGE, “Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2,” Document 2: SNOW 3G Specification, version 10.0.0, 2011.

[4] Biryukov, Priemuth-Schmid and Zhang, “Differential Resynchronization Attacks on Reduced Round SNOW 3G,” ICETE 2010, CCIS 222, pp. 147–157, 2012.

[5] ETSI/SAGE., “Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3, “ Document 2: ZUC specification, V11.0.1., 2012

[6] S. Traboulsi, N. Pohl, J. Hausner, A. Bilgic, and V. Frascolla, “Power analysis and optimization of the ZUC stream cipher for LTE-advanced mobile terminals,” in 2012 IEEE 3rd Latin American Symposium on Circuits and Systems, LASCAS 2012 - Conference Proceedings.

[7] Orhanou, G., & El-Hajji, S., “The New LTE Cryptographic Algorithms EEA3 and EIA3: Verification, Implementation and Analytical Evaluation,” Applied Mathematics and Information Sciences, 7(6), 2385–2390, 2013. http://doi.org/10.12785/amis/070631

[8] Wu, H., Huang, T., Nguyen, P. H., Wang, H., & Ling, S. , “Differential Attacks Against Stream Cipher ZUC,” Advances in Cryptology - ASIACRYPT 2012, LNCS 7658, 262–277, 2012.

[9] G. Kaur and J. Singh, “Data Security using Stream Cipher Algorithm in LTE,” Int. J. Innov. Adv. Comput. Sci., vol. 6, no. 7, pp. 404–408, 2017.

[10] Marton, K., Suciu, A., & Ignat, I., “Randomness in Digital Cryptography: A Survey,” Romanian Journal of Information Science and Technology, 13(3), 219–240, 2010.

[11] SYS, M., RIHA, Z., MATYAS, V., MARTON, K., & SUCIU, A. , “On the Interpretation of Results from the NIST Statistical Test Suite,” Romanian Journal of Information Science and Technology, 18(1), 18–32, 2015.

[12] B. Debraize and I. M. Corbella, “Fault analysis of the stream cipher snow 3G,” in Fault Diagnosis and Tolerance in Cryptography Proceedings of the 6th International Workshop, FDTC 2009, pp. 103–110.

[13] P. Kitsos, G. Selimis and O. Koufopavlou, "High Performance ASIC Implementation of the SNOW 3G Stream Cipher", In IFIP/IEEE VLSI- SOC’08 - International Conference on Very Large Scale Integration, Greece, 2008.

[14] [Lafitte, F., Markowitch, O., & Van Heule, D., “SAT Based Analysis of LTE Stream Cipher ZUC,” Journal of Information Security and Applications, 22, 54–65, 2015. http://doi.org/10.1016/j.jisa.2014.09.004

[15] S. Sen Gupta, A. Chattopadhyay and A. Khalid, "HiPAcc-LTE: An Integrated High Performance Accelerator for 3GPP LTE Stream Ciphers", In INDOCRYPT’11, LNCS, Springer, Vol. 7107, pp. 196–215, 2011.

[16] Wang, L., Jing, J., Liu, Z., Zhang, L., & Pan, W., “Evaluating Optimized Implementations of Stream Cipher ZUC Algorithm on FPGA,” In Lecture Notes in Computer Science (Vol. LNCS 7043, pp. 202–215), (2011). http://doi.org/10.1007/978-3-642-25243-3_17

[17] Doganaksoy, A., Ege, B. , Kocak, O. and Sulak, F., “Cryptographic Randomness Testing of Block Ciphers and Hash Functions,” https://eprint.iacr.org/2010/564.pdf., 2010.

[18] Ahmed, Syed Faiz, et al. "Remote access of SCADA with online video streaming." Computer Science & Education (ICCSE), 2013 8th International Conference on. IEEE, 2013..

[19] Rukhin, A., Soto, J., Nechvatal, J., Miles, S., Barker, E., Leigh, S., … Vo, S., “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” National Institute of Standards and Technology,” Special Publication 800-22, 2010.http://doi.org/10.6028/NIST.SP.800-22r1a

[20] El-etriby, S., Mohamed, E., & Abdul-kader, H., “Modern Encryption Techniques for Cloud Computing: Randomness and Performance Testing,” International Conference on Communications and Information Technology (ICCIT), (March), 800–805, 2012.http://doi.org/10.13140/2.1.4685.8880

[21] Khalid Fadhil Jassim, Imad Fakhri Taha Alshaikhli (2016). Analysis randomness properties of basic components of SNOW 3G cipher in mobile systems. International Journal on Perceptive and Cognitive Computing, 2. , 0 pp. 12-16. ISSN 2462-229