Analysis Randomness Properties of Basic Components of SNOW 3G Cipher in Mobile Systems

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

Department of Computer Science,
Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia
IIUM Cyber Security Malaysia Center for Cyber Space Security
[1]khalid.jassim@yahoo.com, [2]imadf@iium.edu.my

Abstract**—** SNOW 3G is a stream cipher algorithm used as encryption algorithm in third generation mobile phone technology (3G-UMTS). In this paper, we analyzed and evaluated the randomness properties of basic components of SNOW 3G cipher. NIST test suit (SP 800-22) is used in evaluating and testing the randomness properties. We conducted statistical tests on various components of SNOW 3G cipher such as keystream, Finite State Machine, S-boxes S1 and S2, registers (R1, R2, and R3), and Linear Feedback Shift Register. Our experimental results and empirical analysis shown that SNOW 3G cipher passed statistical randomness tests.

Keywords**—** SNOW 3G Cipher, Randomness Tests, Keystream, LFSR, FSM, S-box.

I. Introduction

In the past years, the size of information exchanged via mobile communication systems became huge and more complex. Therefore there was a demand for security of information in different domains. The most suitable tools that offer information confidentiality are cryptographic algorithms. Cryptographic algorithms provide techniques to achieve protection and authentication for the information transmitted through insecure mobile communication networks. Also, these algorithms offer practical methods to protect the exchanged sensitive information and prevent unauthorized parties from reading and accessing this information. Moreover, an important step in the assessment of cryptographic algorithms is to measure the randomness of basic components for these algorithms [1]. In this context, the good randomness of these algorithms leads to remove weaknesses of statistical properties in plaintexts and enhance the security of these algorithms. Furthermore, several statistical randomness tests available in the literatures. For instance, Golomb [2] proposed three postulates to measure randomness properties (runs property, balanced property, and autocorrelation property). More comprehensive randomness tests suits have been proposed such as NIST [3], ENT [4], TestU0 [5], and DIEHARD test [6].

In addition, SNOW 3G stream cipher, as cryptographic algorithm, proposed as confidentiality algorithm in third generation mobile systems (3G-UMTS) [7,8]. This study focused on analyzing and assessing randomness properties of basic components of SNOW 3G cipher algorithm such as keystream, Finite State Machine, S-boxes S1 and S2, registers (R1, R2, and R3), and Linear Feedback Shift Register. The NIST (SP 800-22) statistical test suit has been used in analysis and evaluation process.

This paper is organized as follows. The basic components of SNOW 3G cipher are described in section II. In section III, initialization operation of SNOW 3G stream cipher will be explained. Section IV covers keystream generation mode of SNOW 3G cipher. Section V presents evaluation of randomness properties of SNOW 3G cipher. A discussion of experimental results is given in section VI. Section VII concludes the paper.

II. Components of SNOW 3G Cipher

The SNOW 3G stream cipher depends on two main components, linear feedback shift register (LFSR) and finite state machine (FSM). The register LFSR is based on sixteen stages (S0, S1, … , S15), each stage containing (32- bits), and relies on feedback polynomial defined on finite field GF (2^{32}). The FSM is relied on the registers (R1[32-bit], R2[32-bit], and R3[32-bit]), and includes two substitution boxes (S-box S1, and S-box S2). S-box S1 and S-box S2 are employed to update the contents of registers (R2[32-bit], and R3[32-bit]). Moreover, a secret key (K) of length (128-bit) and initialization variable (IV) of length (128-bit) are used to initialize the components of SNOW 3G cipher. SNOW 3G cipher works in two phases, the first phase includes initialization operation mode and second phase is keysteam generation mode [9,10].

III. SNOW 3G Initialization Operation Mode

The values of secret key K (128-bit) and IV (128-bit) are used to initialize LFSR (S0, S1, … , S15) and registers of FSM (R1[32-bit], R2[32-bit], and R3[32-bit]) [11]. First, the secret key (128-bit) is partitioned into four 32-bit words (k0, k1, k2, and k3). Secondly, the initialization variable IV (128-bit) denoted by the words (IV0[32-bit], IV1[32-bit], IV2[32-bit] and IV3[32-bit]). Then, initialization operation of LFSR as follows:

Let 1 represents the 32-bit word (0xffffffff), and the (xor) denotes bitwise Exclusive-OR operation.

$S_{15} = (k_3 \text{ xor } IV_0)$ $S_{14} = k_2$ $S_{13} = k_1$ $S_{12} = (k_0 \text{ xor } IV_1)$
$S_{11} = (k_3 \text{ xor } 1)$ $S_{10}=(k_2 \text{ xor } 1 \text{ xor } IV_2)$ $S_9 = (k_1 \text{ xor } 1V_3)$
$S_8 = (k_0 \text{ xor } 1)$ $S_7 = k_3$ $S_6= k_2$ $S_5 = k_1$ $S_4 = k_0$
$S_3 = (k_3 \text{ xor } 1)$ $S_2= (k_2 \text{ xor } 1)$ $S_1 = (k_1 \text{ xor } 1)$ $S_0 = (k_0 \text{ xor } 1)$

Moreover, the three registers of FSM initialized with zero (R1=0, R2=0, and R3=0). Then, SNOW 3G cipher clocks 32 times without generating keystream [12].

```
Repeat Step#1 and Step#2 32 times
{
  Step#1: The registers of FSM are clocked to generate F
          (32-bit word).
          F = ((S15 ⊞ R1) xor R2), (The operation ⊞ means
              addition mod $2^{32}$ )
          r = (R2 ⊞ (R3 xor S5))
          R3 = Sbox-S2 [R2], R2 = Sbox-S1[R1], and R1 = r.

  Step#2: Then the stages of LFSR are shifted and using F
          (32-bit word).
          V = (S0,1 || S0,2 || S0,3 || 0x00) xor MULα(S0,0)
              xor S2 xor (0x00 || S11,0 || S11,1 || S11,2) xor
              DIVα (S11,3) xor F.
          S0 = S1, S1 = S2 , … , S14 = S15, and S15 = V.
}
```

IV. SNOW 3G Keystream Generation Mode

In keystream generation mode (Figure 1) [13], the components of FSM are clocked (as below in Step#1) one time and at the same time ignoring the 32-bit output of FSM. Then, the stages of LFSR are clocked one time using keystream mode (as below in Step#3). Moreover, SNOW 3G generates keystream of n words (32-bit) [11, 14] as follows:

```
For t= 1 to n
{
  Step#1: The components of FSM are clocked and generate
          output F (F=32-bit word).
          F = ((S15 ⊞ R1) xor R2), ( ⊞: means addition mod
              $2^{32}$ )
          r = (R2 ⊞ (R3 xor S5))
          R3 = Sbox-S2 [R2], R2 = Sbox-S1[R1], and R1 = r.
  Step#2: Calculate $Z_t$, which is the next 32-bit word of
          output keystream.
          $Z_t$ = (F xor S0)
  Step#3: Then stages of register (LFSR) shifted by using
          keystream mode.
          V = (S0,1 || S0,2 || S0,3 || 0x00) xor MULα(S0,0)
              xor S2 xor (0x00 || S11,0 || S11,1 || S11,2) xor
              DIVα (S11,3).
          S0 = S1, S1 = S2, … , S14 = S15 , and S15 = V.
}
```

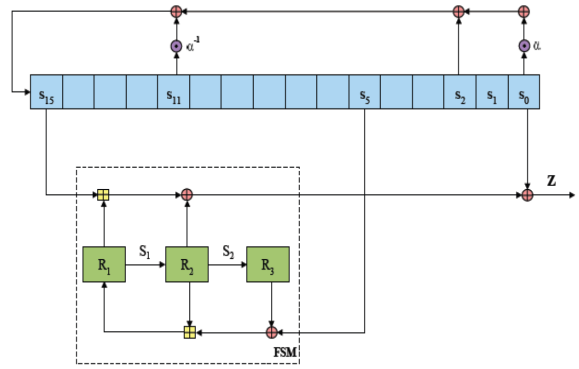


Fig. 1 SNOW 3G Cipher.

V. Randomness Properties of SNOW 3G Cipher

The statistical test suit NIST (SP 800-22) may be used to compute randomness properties of generated sequences and keystreams [15, 16]. The NIST test suit contains a number of statistical tests (Table 1 and Table 2). Moreover, the approach of testing statistical hypothesis is used in NIST test suit and to evaluate the null hypothesis (H0). H0 means the generated sequence, or keystream, is random as assumed in NIST test suit. The parameter (α) is selected to represent significance level in NIST statistical tests [17]. Each of the statistical tests will produce p-value (0≤ p ≤1, as real numbers). If the computed p-value p < α then H0 is rejected and it means the generated sequence is not random. But, if p ≥ α then H0 is accepted and in this case the generated sequence is random. For all the statistical tests in this research, level of significance (α = 0.01) [18, 19].

Furthermore, the NIST test suit was used to evaluate randomness properties of basic components of SNOW 3G cipher algorithm. We used a sample size (S=100) of generated sequences and keystreams, with length (n=1 Mega bit, or $n=2^{20}$), and different keys (Ks) and initialization variables (IVs). Also, in our analysis study the parameters for the NIST test suit have been defined as follows:

- Block length of Block Frequency test (M=128).
- Block length of Non Overlapping Template test (m=9).
- Block length of Overlapping Template test (m=9).
- Block length of Approximate Entropy test (m=10).
- Block length of Serial test (m=16).
- Block length of Linear Complexity test (M=500).
- Sequence Length, or length of keystreams ($n =2^{20}$)
- Sample Size, or number of sequences and keystreams (S=100).
- Significance Level (α=0.01).

VI. Experimental Results

The NIST statistical tests of randomness were performed on (100) sequences and keystreams generated by simulation software program of SNOW 3G cipher algorithm. The results of NIST statistical tests are shown in Table 1 and Table 2. First column of (Table 1 and Table 2) represents NIST statistical tests. For each test, NIST test suit computes p-value for each sequence and keystream. A sequence and keystream pass a test when its p-value ≥ 0.01.

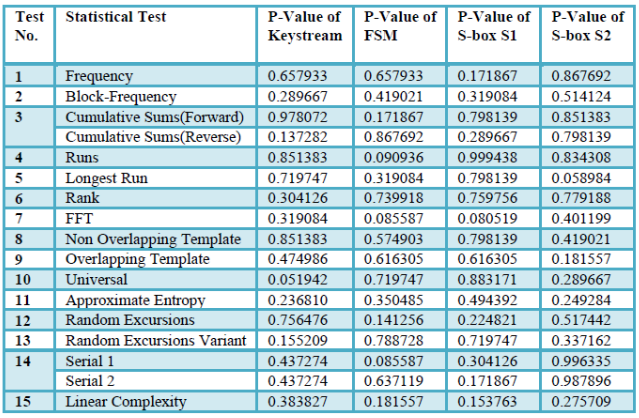
In our evaluation of randomness properties we shall use the following classification:

- In general, the lowest p-values of tests represent the low randomness of sequences and the high p-values indicate better randomness properties [3].
- If the p-values of some tests are ($p < 0.01$) then the result is fail randomness.
- If the p-values are ($0.01 \le p < 0.50$) in majority of tests then the randomness is low.
- If the p-values are ($0.50 \le p < 1$) in majority of tests then the randomness is high.
- If the p-values are ($0.01 \le p < 0.50$) in 8 or 9 tests, or p-values are ($0.50 \le p < 1$) in 8 or 9 tests then the randomness is moderate.

The randomness of basic components of SNOW3G cipher has been analysed and the results as follows:

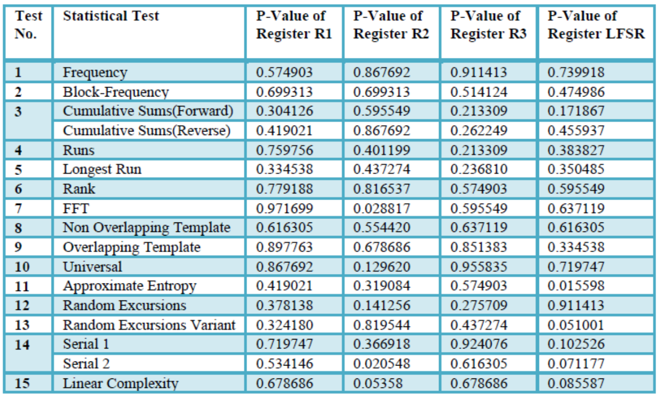
- The p-value of keystream (Table 1) was high in Cumulative Sums (Forward) test (0.978072) and the lowest p-value was (0.051942) in Universal test. Moreover, the p-values out of (17) tests, in (11) tests were less than (0.50). Which indicate low randomness for keystream (Figure 2).
- For output sequence of Finite State Machine (FSM, Table 1), the highest p-value noticed in Cumulative Sums (Reverse) test (0.867692), where FFT test and Serial 1 test registered lowest p-value (0.085587). In addition, the p-values in (8) tests were greater than (0.50) which denote moderate randomness for FSM (Figure 3).
- For output sequence of S-box S1 (Table 1), the minimum value showed in FFT test (0.080519) and maximum value was in Runs test (0.999438). Furthermore, the p-values were greater than (0.50) in (8) tests which point out moderate randomness for output sequence of S-box S1 (Figure 4).
- For output sequence of S-box S2 (Table 1), the lowest value (0.058984) observed in Longest Run test and highest value (0.996335) was in Serial 1 test. Also, the p-values were greater than (0.50) in (9) tests which signify moderate randomness for output sequence of S-box S2 (Figure 5).
- The highest p-value of Register R1 (Table 2) was (0.971699) in FFT test and lowest was (0.304126) in Cumulative Sums (Forward) test. However, the p-values were greater than (0.50) in (11) tests which show high randomness for Register R1 (Figure 6).
- In Register R2 (Table 2), the highest value (0.867692) noticed in Frequency and Cumulative Sums (Reverse) tests, and lowest value was (0.020548) in Serial 2 test. On the other hand, the p-values were less than (0.50) in (9) tests which reveal moderate randomness for Register R2 (Figure 7).
- For Register R3 (Table 2), the highest value (0.955835) observed in Universal test and lowest value was (0.213309) in Cumulative Sums (Forward) and Runs tests. Besides, the p-values were greater than (0.50) in (11) tests which mean high randomness for Register R3 (Figure 8).
- In Register LFSR (Table 2), the highest value (0.911413) introduced in Random Excursions test and lowest value was (0.015598) in Approximate Entropy test. Also, the p-values were less than (0.50) in (11) tests which indicate low randomness for Register LFSR (Figure 9).
- In overall, the basic components of SNOW 3G have passed the various statistical tests.

TABLE1
Randomness Results of Keystream, FSM, S-box S1, and S-box S2.



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	0.798139	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 Excursions 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 2
Randomness Results of Registers R1, R2, R3, and LFSR



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	0.867692	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	0.378138	0.141256	0.275709	0.911413
13	Random Excursions Variant	0.324180	0.819544	0.437274	0.051001
14	Serial 1	0.719747	0.366918	0.924076	0.102526
	Serial 2	0.534146	0.020548	0.616305	0.071177
15	Linear Complexity	0.678686	0.05358	0.678686	0.085587

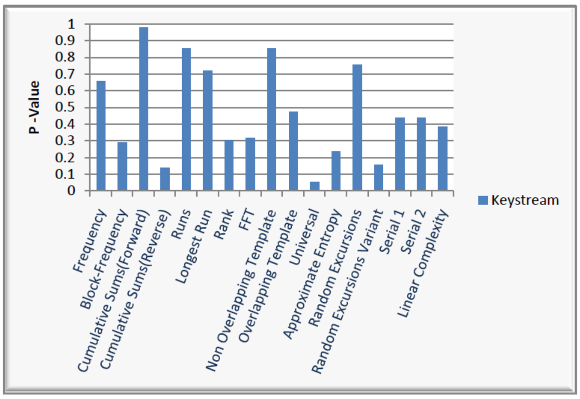


Fig. 2 Randomness Tests of Keystream

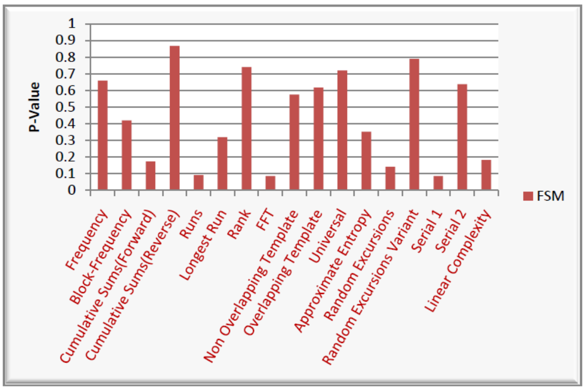


Fig.3 Randomness Tests of Output Sequence of Finite State Machine

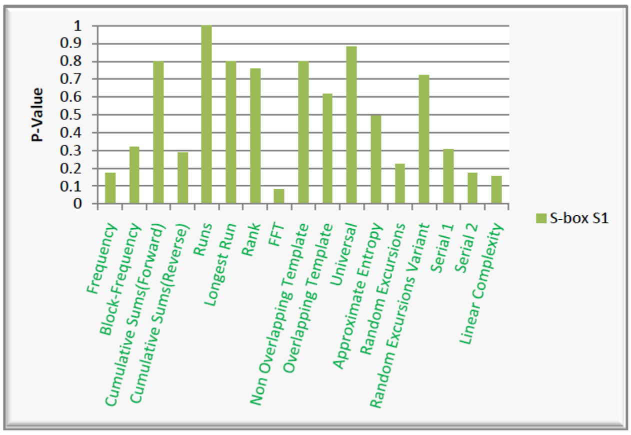


Fig. 4 Randomness Tests of Output Sequence of S-box S1

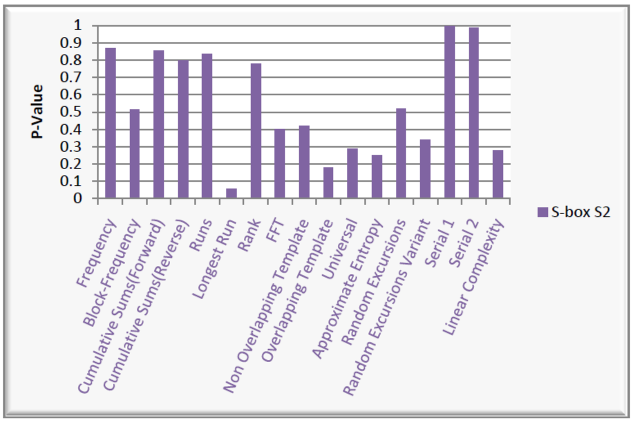


Fig.5 Randomness Tests of Output Sequence of S-box S2

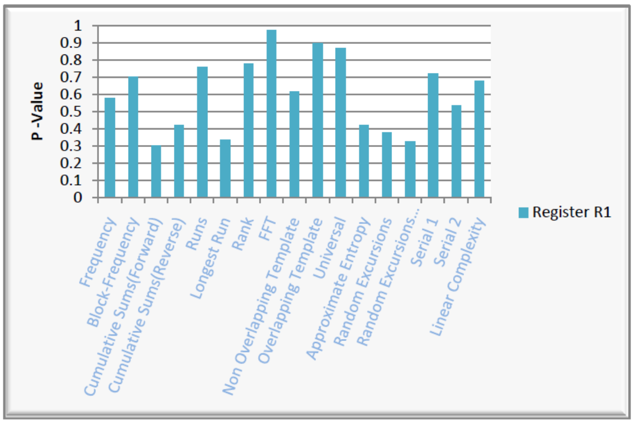


Fig. 6 Randomness Tests of Output Sequence of Register R1

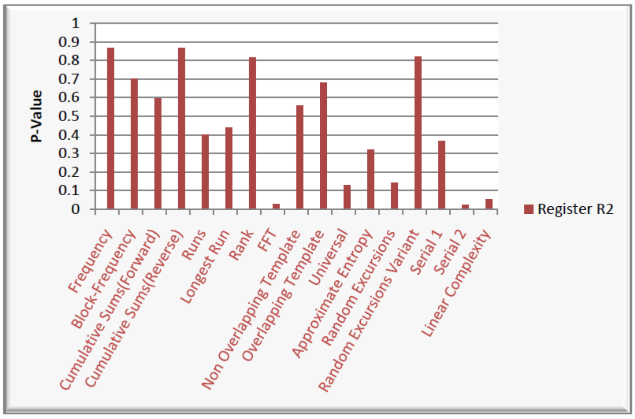


Fig. 7 Randomness Tests of Output Sequence of Register R2

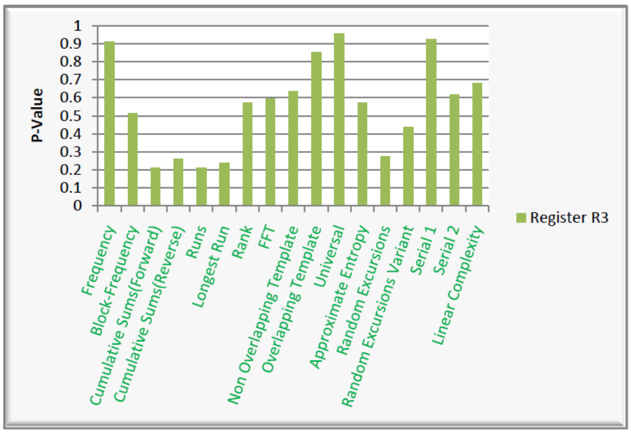


Fig. 8 Randomness Tests of Output Sequence of Register R3

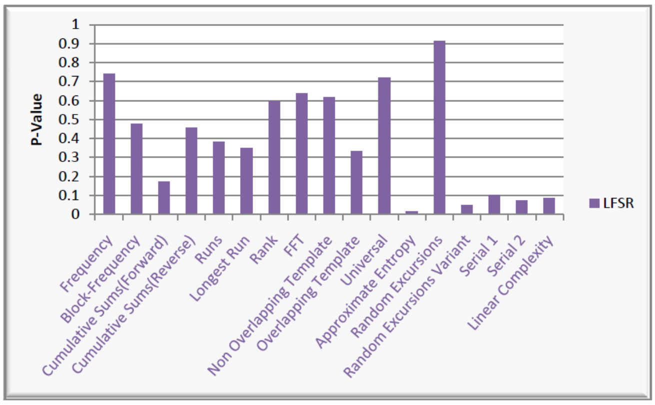


Fig. 9 Randomness Tests of Output Sequence of Linear Feedback Shift Register

VII. Conclusions

This paper provides analysis study of randomness properties of SNOW 3G cipher. The statistical test suit (NIST) has been used to assess randomness properties of this cipher. Experimental results have shown that keystream and register LFSR possess low randomness. Also, output sequences of FSM, S-box S1, S-box S2, and register R2 have moderate randomness. However, output sequences of registers R1 and R3 possess high randomness. In over all, the basic components of SNOW 3G cipher have passed statistical randomness tests.

References

[1] Cristina-Loredana Duta, Bogdan-Costel Mocanu, Florin-Alexandru Vladescu and Laura Gheorghe, “Randomness Evaluation Framework of Cryptographic Algorithms”, International Journal on Cryptography and Information Security (IJCIS), Vol. 4, No. 1, March 2014.

[2] S. W. Golomb, “Shift Register Sequences”, Aegean Park Press, Laguna Hills, CA, USA, 1981.

[3] National Institute of Standards and Technology, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, Special publication 800-22, April 2010.

[4] J. Walker, “ENT – A pseudorandom number sequence test program”, 2008, available at http://www.fourmilab.ch/random/ (Accessed: March 2016).

[5] P. L'Ecuyer and R. Simard, “TestU01: A C library for empirical testing of random number generators”, in ACM Transactions on Mathematical Software, 2007.

[6] G. Marsaglia, "DIEHARD Battery of Tests of Randomness [Online]", Available at http://www.stat.fsu.edu/pub/diehard.

[7] Synopsys Inc., "CLP-41: SNOW 3G Flow Through Core", Available at http://www.synopsys.com/IP/security-ip/cryptographic-cores/Pages/clp-41.aspx, Retrieved on February 2016.

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

[9] *P. Ekdahl and T. Johansson, "A New Version of the Stream Cipher SNOW", In Selected Areas in Cryptography (SAC'02), LNCS, Springer,* Vol. 2595, pp. 47–61, 2003.

[10] ETSI/SAGE, “Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2,” Document 5: Design and Evaluation Report, version 1.1, 2006.

[11] 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.

[12] B. Debraize and I.M. Corbella, " Fault Analysis of the Stream Cipher Snow 3G", In Fault Diagnosis and Tolerance in Cryptography (FDTC'09), September, 2009.

[13] 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.

[14] IP Cores Inc., " SNOW 3G LTE Encryption IP Core", Available at http://www.ipcores.com/Snow3G.htm. Retrieved on February 2016.

[15] M. S. Turan, A. Doğanaksoy and C. Calik, “Statistical Analysis of Synchronous Stream Ciphers”, in Proceedings of SASC 2006: Stream Ciphers Revisited, 2006.

[16] J. Soto, “Randomness testing of the AES candidate algorithms”, 1999, http://csrc.nist.gov/encryption/aes/round1/r1-rand.pdf.

[17] J. Soto, “Statistical Testing of Random Number Generators”, 1999, http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf

[18] Ali Doganaksoy, Barıs Ege, Onur Kocak and Fatih Sulak,"Cryptographic Randomness Testing of Block Ciphers and Hash Functions", https://eprint.iacr.org/2010/564.pdf.

[19] D. Biebighauser, "Testing Random Number Generators", 2000, http://www.math.umn.edu/~garrett/students/reu/pRNGs.pdf.