"Constantin Brâncuşi" University of Târgu Jiu ENGINEERING FACULTY
SCIENTIFIC CONFERENCE – 13 th edition – with international participation
November 07-08, 2008 – Târgu Jiu

STATISTICAL EVALUATION OF STREAM CIPHER SNOW 3G

Mgr. Patrik Böhm

Department of Quantitative Methods and Informatics,
Faculty of Operation and Economics of Transport and Communications, University of Žilina, Slovak Republic

ABSTRACT:

In January 2006, ETSI/SAGE released specifications of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2, which are used in mobile communications systems. Since then, several security evaluations of these algorithms were published. In our paper we deal with statistical properties of stream cipher SNOW 3G, which is the core part of both algorithms.

1 Introduction

The development of the second phase of 3GPP confidentiality and integrity algorithms was undertaken in response to an initiative from GSMA Security Group. Even though there are not any indications of weaknesses in the previous version of algorithms, the new algorithms are fundamentally different from previous, so that the attack on one algorithm is unlikely to translate into an attack on another [1].

New algorithms are based on stream cipher (keystream generator) SNOW 3G, which is a modified version of SNOW 2.0

1.1 Specification of SNOW 3G cipher

Cipher SNOW 3G is synchronnous aditive stream cipher. Its key size is 128 bits, initialization vector (IV) has 128 bits. Algorithm starts with initialization of the cipher componenets based on the values of key and IV. The schema if the cipher is on the *Figure 1*. Cipher consists of two components, linear feedback register of length 16 over finite field F_2^{32} and finite state machine (FSM). Detailed specification of the cipher can be found in [2].

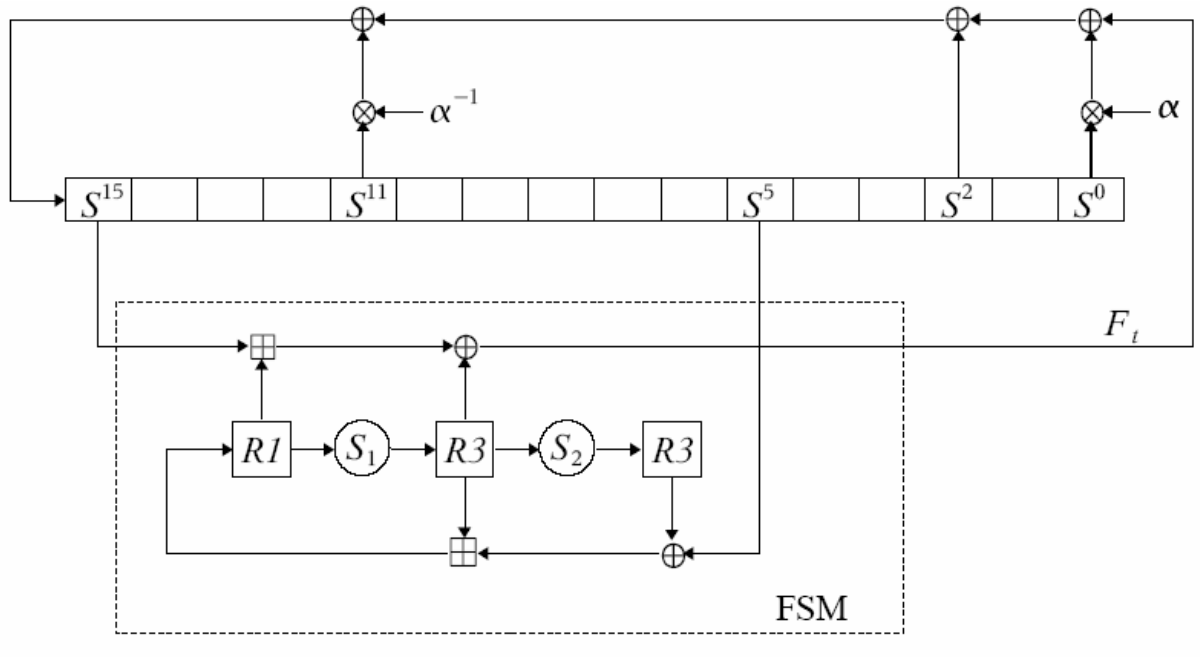


Figure 1

1.2 Randomness testing

Statistical testing has always been a basic part of evaluation of block ciphers. For example, randomness testing was used during the evaluation of Advanced Encryption Standard (AES) [3]. Statistical testing is only one part of the security criteria, but it may provide usefull inital classification of algorithms. Failing from these tests means that the cipher doesn't pass basic security requirements. However, passing the statistical tests does not guarantee that the cipher is rsistant to other attacks.

Various tests suits are commonly used:

- DIEHARD [4] battery of tests consists of 18 independent statistical randomness tests
- Crypt-X [5] is a comprehensive software package which includes 6 efficient tests
- NIST [6] statistical test suite consists of 15tests.
- NESSIE [7] proposed their own statisticaltoolbox, which is small variation of NIST statistical test suite

In our research we have chosen NIST statistical test suite. Here is a list of statistical tests included: frequency (monobit) test, frequency test within a block, runs test, test for the longest run of ones in a block, binary matrix rank test, discrete Fourier transform (spectral) test, non-overlapping and overlapping template matching test, Maurer's „universal statistical“ test, linear complexity test, serial test, approximate entropy test, cumulative sums (cusums) test, random excursion test and random excursion variant test.

For each experiment, the significance level was set to 0.01, sample size was set to 300 sequences.

2 Proposed tests

I proposed three statistical tests to evaluate randomness properties of keystream generator part of SNOW 3G cipher. The tests were motivated by randomness testing of AES candidates [3], [8].

Long keystream data set.

The purpose of this test is to evaluate the randomness of long keystream generated by the algorithm. $2^{20} = 1048576$ bits of keystream are generated for each of 300 randomly chosen keys. IV is set zero.

Short keystream data set.

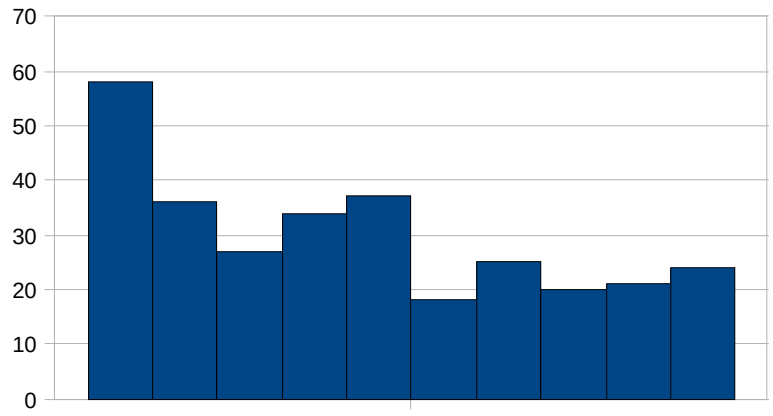
The purpose of this test is to evaluate the randomness of short keystream generated by the algorithm. $2^{10} = 1024$ bits of keystream are generated for each of 307,200 randomly chosen keys. IV is set zero. 1024 generated keystreams are concatenated to form 300 blocks, each consisting of 1,048,576 bits.

IV data set.

The purpose of this test is to evaluate the correlation between different values of IV. 300 data sets are generated from randomly chosen keys. Each data set is a concatenation of 256 sequences, each 4096 bits long. First keystream sequence is generated with zero IV, following 255 keystreams are generated with IV each time incremented by one.

3 Empirical results

Cipher SNOW 3G has passed all the tests for *Long keystream data set* and *IV data set*. These tests have not disclosed any deviations from randomness. On the contrary, the cipher has not passed eight tests for *Short keystream data set:* runs test, test for the longest run of ones in a block, binary matrix rank test, discrete Fourier transform (spectral) test, non-overlapping template matching test, overlapping template matching test, approximate entropy test and serial test. All of these tests have not satisfied the uniformity of P-values. As an example of distribution of P-values, we present *Graph 1*, were P-values for block-frequency test are drawn. The visual impression that the distribution is not symmetric can be verified by goodness of fit test, for example.



Graph 1

It suggests that the first 1024 bits of keystream could be distinguished from the random sequence.

Conclusions

In our research we have performed statistical tests on three data sets generated by the cipher SNOW 3G. IV data set has not passed eight out of fifteen tests, which suggests that there is weakness in the initialization of the cipher. More research should be done to prove or refuse our assumption.

It is necessary to note that the eventual weaknesses in SNOW 3G algorithm doesn't necessarily imply any weaknesses in 3GPP confidentiality and integrity algorithms, since we supposed zero IV in all tests, which is never true in UEA2 and UIA2 algorithms.

Bibliography

[1] ETSI/SAGE Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification, version 1.1., http://www.gsmworld.com/using/algorithms/docs/etsi_sage_06_09_06.pdf

[2] ETSI/SAGE Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification, version 1.1., http://www.gsmworld.com/using/algorithms/docs/snow_3g_spec.pdf

[3] Soto, J.: Randomness Testing of the AES Candidate Algorithms, NIST 1999, http://csrc.nist.gov/encryption/aes/round1/r1-rand.pdf

[4] Marsaglia, G.:DIEHARD Battery of Tests of Randomness. http://stat.fsu.edu/~geo/diehard.html

[5] Information Security Institute, Crypt-X, 1998. http://www.isi.qut.edu.au/resources/cryptx

[6] Rukhin, A. et al.: A Statistical Test Suite for the Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22 2001, http://csrc.nist.gov/rng/SP800-22b.pdf

[7] New European Schemes for Signatures, Integrity, and Encryption (NESSIE), http://www.cryptonessie.org.

[8] Bohm, P.: Statistical properties of stream ciphers submitted to ECRYPT e-stream project, In: ELITECH´06 - S. 1/3-8/3