UDC 004.056.55

STATISTICAL PROPERTIES OF MODERN STREAM CIPHERS

Oleksii Nariezhnii, Egor Eremin, Vladislav Frolenko, Kyrylo Chernov, Tetiana Kuznetsova, Yevhen Demenko

V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
o.nariezhnii@karazin.ua, suvenick2@gmail.com, jadson27101@gmail.com, kirillfilippsky@gmail.com, kuznetsova.tatiana17@gmail.com, demenjay@gmail.com

Reviewer: Ivan Gorbenko, Doctor of Sciences (Engineering), Full Professor, Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
gorbenkoi@iit.kharkov.ua

Received on September 2018

Abstract. *In recent years, numerous studies of stream symmetric ciphers in Ukraine are continuing, the main purpose of which is to argue the principles of creating a new cryptographic algorithm, which can be based on the national standard. One of the essential aspects in choosing from many alternatives is the statistical properties of the output pseudorandom sequence (key stream). In this paper, the results of comparative studies of statistical properties of output sequences, which are formed by various stream ciphers, in particular, by world-known algorithms Enocoro, Decim, Grain, HC, MUGI, Mickey, Rabbit, RC-4, Salsa20, SNOW2.0, Sosemanuk, Trivium and the Ukrainian cryptographic algorithm Strumok, that was developed in recent years, are presented. For comparative studies, the NIST STS method was used, according to which experimental studies are performed in 15 statistical tests, the purpose of which is to determine the randomness of the output binary sequences. Each of the tests is aimed at studying certain vulnerabilities of the generator, that is, points to the potential usage of different methods of cryptographic analysis. Although each of the considered streaming encryption algorithms has been studied, we have carried out a statistical test of the generated pseudorandom sequences under equal conditions and with identical initial parameters, that is, our results allow us to perform a comparative analysis of ciphers and to justify the best of statistical properties. The estimates presented in the article, as expected, confirmed the high statistical security indexes of modern ciphers. In addition, according to the results of experimental research, it was found that the new Ukrainian development - the stream cipher Strumok does not yield to the best world algorithms in the statistical properties of the initial sequences*.

Keywords: *symmetric cryptography; stream cryptographic algorithms; gamma; cryptanalysis; statistical tests.*

1 Introduction

Nowadays, there is a large number of areas in technology where it is necessary to use cryptography to protect information. These areas include Internet of things (IoT), smart sensors and controllers, medical devices, RFID tags. That is why in the modern world different requirements for crypto algorithms are formed, however there is one common requirement – it is stability.

The stability of the stream cryptosystem depends very much on the quality of the generated gamma, because if the gamma is predictable, the space of the possible keys will be smaller and it will be possible to go through all values. Determining the randomness of the generated sequences is one of the main tasks.

Generating random numbers means getting a sequence of binary characters 0 and 1. Pseudorandom sequence generators are a function that is initialized by the seed, and then generate a sequence 0 and 1 at the output. Knowing this seed, we can predict the entire sequence. A good PRNG generator is one for which it is impossible to predict the following values, with having all the history of the previous values without having the seed [1].

This article is dedicated to the study of statistical properties of pseudorandom sequences, which are formed by different streaming cryptographic algorithms.

For conducting experimental studies, world-known stream symmetric ciphers that were standardized at the international and/or national level or presented in various research projects, for example, at the international eSTREAM competition, were involved. In particular, we reviewed the specification and developed the software implementation of stream ciphers Enocoro, Decim, Grain, HC, MUGI, Mickey, Rabbit, RC-4, Salsa20, SNOW2.0, Sosemanuk, Trivium [2-7]. The Ukrainian stream cipher Strumok, which was developed and presented in [8] and subsequently improved several times and researched [9-13], was involved to studies in addition. In particular, in our last paper

[13] the same streaming cryptographic algorithms were considered, but we carried out a comparative analysis of the computational complexity of stream ciphers and their performance on various computing systems.

The test of the National Institute of Standards and Technology (NIST) of the USA «A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications» (STS) [1] was used in this work to conduct comparative experimental studies of the statistical properties of output pseudorandom sequences. This method has been developed and tested in the study of candidates for the national standard of block symmetric ciphers in the United States (the winner and published as standard [14], as is known, was the algorithm Rijndael).

The NIST STS method consists of 15 independent statistical tests, although, depending on individual parameters and settings, 188 statistical tests are usually performed. The basis of all these tests is the concept of zero hypothesis. Zero hypothesis is the assumption that there is no relationship between the two facts. There is also an alternative hypothesis that refutes the null hypothesis: that is, there is an interconnection between facts. If we proceed to the terms of random numbers, then for the null hypothesis assumes that the sequence is truly random (whose values appear equip probable and independently of each other). Consequently, if the null hypothesis is correct, then our generator produces sufficiently "good" random numbers [1]. For each test, we need to select the appropriate random statistics and use it to determine whether or not to accept the null hypothesis. With the assumption of randomness, such statistics have a distribution of possible values. The theoretical proof of the distribution of this statistics for a zero hypothesis is determined by mathematical methods. During the test, the value of the statistic for the data (the test sequence) is calculated. This statistic value of the test is compared with the critical value. If the value of the statistical test exceeds the critical value, the null hypothesis of randomness is rejected. Otherwise, the null hypothesis (the hypothesis of randomness) does not deviate (that is, the hypothesis is accepted) [1].

Of course, chosen cryptographic transformations Enocoro, Decim, Grain, HC, Mugi, Mickey, Rabbit, RC-4, Salsa20, SNOW2.0, Sosemanuk and Trivium have been repeatedly tested, including by developers [2-7]. But all these studies were performed on different platforms with different settings and output parameters. That is, the statistical properties of the initial sequences of each algorithm (*with their own settings*) were studied without conducting a comparative analysis of the statistical safety indicators and the justification of the best cipher according to the statistical properties.

The purpose of our work is to independently test the properties of cryptographic algorithms from [2-7] with universal and identical conditions in order to obtain objective and independent results. Special attention was paid to the streaming encryption algorithm Strumok, which was developed and presented by Ukrainian scientists in [8-13]. To date, numerous studies have been conducted in Ukraine to substantiate the principles of creating a new streaming cryptographic algorithm, which may be the base of the national standard. Therefore, experimental studies of the statistical properties of the Strumok algorithm, their comparative analysis with the value of statistical security of world-known ciphers from [2-7] is undoubtedly relevant and important scientific task.

2 Researched Symmetric Ciphers and Testing Conditions

During conducting of experimental researches modern stream symmetric ciphers were considered: Enocoro [2,3], Decim [2,6], Grain [7], HC [7], MUGI [2], Mickey [7], Rabbit [2,7], RC-4 [7], Salsa20 [7], SNOW2.0 [2], Sosemanuk [7], Trivium [2], Strumok [8,11], also block encryption algorithm AES [14,15], which can be used in streaming encryption modes.

The list of studied algorithms is given in Table 1, which provides brief information about ciphers and affiliation with relevant standards or research projects.

For testing were developed software implementation of all the studied stream ciphers in Java language. For each crypto algorithm, sequences of size of one million bits and ten thousand bits were generated with the help of a randomly generated key. These sequences have been tested on a single platform by tests on randomness.

These tests focus on a types of non-randomness that can exist in the sequence.

Table 1 – The Chosen Crypto Algorithms For Comparison

The name of the cipher	Source of specification	State size, bit	Key size, bit	Size IV, bit
AES	FIPS-197, CRYPTREC, ISO/IEC 18033-4	128	128, 256	256
Enocoro	ISO/IEC 29192-3	272	80, 128	64
DECIMv2	ISO/IEC 18033-4, eSTREAM	288	128	128
GRAIN	eSTREAM	128	128	96
HC	eSTREAM	128, 256	128, 256	128, 256
MUGI	ISO/IEC 18033-4	128	128	128
MICKEY	eSTREAM	160	128	128
Rabbit	ISO/IEC 18033-4, eSTREAM	513	128	64
RC4	Mailing list Cypherpunks	256	256	–
SALSA-20	eSTREAM	512	128	64
SNOW2.0	ISO/IEC 18033-4	512	128, 256	128, 56
SOSEMANUK	eSTREAM	512	128	128
TRIVIUM	eSTREAM, ISO/IEC 29192-3	288	80	80
Strumok-256	[8, 11]	1024	256	256
Strumok-512		1024	512	512

These tests are included: The Frequency (Monobit) Test, Frequency Test within a Block, The Runs Test, Tests for the Longest-Run-of-Ones in a Block, The Binary Matrix Rank Test, The Discrete Fourier Transform (Spectral) Test, The Non-overlapping Template Matching Test, The Overlapping Template Matching Test, Maurer's "Universal Statistical" Test, The Linear Complexity Test, The Serial Test, The Approximate Entropy Test, The Cumulative Sums (Cusums) Test, The Random Excursions Test, and The Random Excursions Variant Test [1].

For all tests, the rule of acceptance the randomness is as follows: if the computed P-value is < 0.01, then conclude that the sequence is non-random. Otherwise, conclude that the sequence is random [1].

Randomness tests were implemented in Python. For each test, a quantitative probability characteristic was obtained, these values were studied and analyzed. The experimental results obtained from each test were compared with the value of the criterion of significance (which is equal to 0.01, that is, it is a probability to reject the correct zero hypothesis by mistake).

3 Results of Statistical Tests

The results of NIST testing are shown in Tables 2-16.

Results of The Frequency (Monobit) Test and Results of Frequency Test within a Block (Table 2, 3) can be interpreted as follows: the closer the value of P-value to 1 is more evenly distributed "0" and "1". A small value of P-value means a large deviation from the equable distribution of zeros and ones in at least one of the sequence blocks. That is, the smaller the value, the more unevenly distributed values.

Table 2 – Results of The Frequency (Monobit) Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.52217	Rabbit	0.92034
AES-256	0.98404	RC4	0.01046
Enocoro	0.20054	SALSA-20	0.33705
DECIM v2	0.52217	SNOW2.0-128	0.81033

Continuation of Table 2

GRAIN	0.20059	SNOW2.0-256	0.14986
HC -128	0.14429	SOSEMANUK	0.07840
HC -256	0.48392	TRIVIUM	0.50925
MUGI	0.92034	Strumok-256	1.0
MICKEY	0.49650	Strumok-512	0.14135

Table 3 – Results of the Frequency Test within a Block

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.35359	Rabbit	0.46658
AES-256	0.25300	RC4	0.50833
Enocoro	0.39109	SALSA-20	0.71156
DECIM v2	0.33150	SNOW2.0-128	0.86422
GRAIN	0.64794	SNOW2.0-256	0.06933
HC -128	0.96846	SOSEMANUK	0.72974
HC -256	0.92374	TRIVIUM	0.51628
MUGI	0.40069	Strumok-256	0.75319
MICKEY	0.64356	Strumok-512	0.36249

Table 4 – Result of the Runs Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.12254	Rabbit	0.23795
AES-256	0.54850	RC4	0.70787
Enocoro	0.06926	SALSA-20	0.97669
DECIM v2	0.39203	SNOW2.0-128	0.28887
GRAIN	0.51188	SNOW2.0-256	0.96867
HC -128	0.65891	SOSEMANUK	0.34245
HC -256	0.07756	TRIVIUM	0.17519
MUGI	0.77940	Strumok-256	0.71884
MICKEY	0.23191	Strumok-512	0.56320

Table 5 – Results of Tests for the Longest-Run-of-Ones in a Block

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.56531	Rabbit	0.30447
AES-256	0.31757	RC4	0.60474
Enocoro	0.32566	SALSA-20	0.54449
DECIM v2	0.45269	SNOW2.0-128	0.21839
GRAIN	0.46634	SNOW2.0-256	0.59095
HC -128	0.22625	SOSEMANUK	0.17928
HC -256	0.50297	TRIVIUM	0.12140
MUGI	0.18882	Strumok-256	0.61075
MICKEY	0.16730	Strumok-512	0.24879

Table 6 – Results of the Binary Matrix Rank Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.62395	Rabbit	0.53858
AES-256	0.34227	RC4	0.37364
Enocoro	0.42643	SALSA-20	0.62596
DECIM v2	0.53868	SNOW2.0-128	0.42577

Continuation of Table 6

GRAIN	0.25851	SNOW2.0-256	0.56234
HC -128	0.35643	SOSEMANUK	0.23127
HC -256	0.63508	TRIVIUM	0.32610
MUGI	0.25313	Strumok-256	0.77838
MICKEY	0.43287	Strumok-512	0.43683

Table 7 – Results of the Discrete Fourier Transform (Spectral) Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.58190	Rabbit	0.78308
AES-256	0.40886	RC4	0.58190
Enocoro	0.46286	SALSA-20	0.19888
DECIM v2	0.04350	SNOW2.0-128	0.40886
GRAIN	0.77958	SNOW2.0-256	0.82688
HC -128	0.58190	SOSEMANUK	0.71357
HC -256	0.14203	TRIVIUM	0.92688
MUGI	1.0	Strumok-256	0.47081
MICKEY	0.40886	Strumok-512	0.58190

Table 8 – Results of the Non-overlapping Template Matching Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.88179	Rabbit	0.53417
AES-256	0.58654	RC4	0.74029
Enocoro	0.32005	SALSA-20	0.51304
DECIM v2	0.51093	SNOW2.0-128	0.29576
GRAIN	0.03834	SNOW2.0-256	0.98602
HC -128	0.72360	SOSEMANUK	0.71631
HC -256	0.66453	TRIVIUM	0.61436
MUGI	0.57822	Strumok-256	0.88153
MICKEY	0.70717	Strumok-512	0.70137

The smaller the value of P-value for the Runs Test (Table 4) the smaller the number of changes of the value in the sequence. Fluctuations should be approximately equal to the expected fluctuations in completely random sequences.

The greater the value of P-value for the greater the value of P-value (Table 5) the more evenly distributed cluster ones in the sequence. The small values of the P-value for the Binary Matrix Rank Test (Table 6) indicate that there is a deviation of the rank distribution from what corresponds to the random sequence. With a low value of the P-value for The Discrete Fourier Transform (Spectral) Test (Table 7), we can conclude that in the sequence there are too many peaks that exceed the threshold in the sequence if it was random.

If the P-value is too small for The Overlapping Template Matching Test (Table 9), then in sequence there is an excess of defined value patterns. According to the results of this test, we can also say if there are too many single defined patterns in the sequence. This will be visible if the P-value is too small.

Table 9 – Results of the Overlapping Template Matching Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.63467	Rabbit	0.46289
AES-256	0.42685	RC4	0.64860
Enocoro	0.35152	SALSA-20	0.49497

Continuation of Table 9

DECIM v2	0.52759	SNOW2.0-128	0.64848
GRAIN	0.24286	SNOW2.0-256	0.52567
HC -128	0.58395	SOSEMANUK	0.64954
HC -256	0.75296	TRIVIUM	0.38551
MUGI	0.48632	Strumok-256	0.83526
MICKEY	0.63858	Strumok-512	0.53734

Table 10 – Results of the Maurer's "Universal Statistical" Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.72412	Rabbit	0.48576
AES-256	0.52788	RC4	0.40352
Enocoro	0.32640	SALSA-20	0.73056
DECIM v2	0.42902	SNOW2.0-128	0.58112
GRAIN	0.57329	SNOW2.0-256	0.68674
HC -128	0.66285	SOSEMANUK	0.59053
HC -256	0.42758	TRIVIUM	0.48921
MUGI	0.74892	Strumok-256	0.64992
MICKEY	0.67342	Strumok-512	0.57924

Table 11 – Results of the Linear Complexity Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.68768	Rabbit	0.36868
AES-256	0.65642	RC4	0.56226
Enocoro	0.86532	SALSA-20	0.35788
DECIM v2	0.46743	SNOW2.0-128	0.38573
GRAIN	0.44180	SNOW2.0-256	0.57693
HC -128	0.45474	SOSEMANUK	0.45798
HC -256	0.64957	TRIVIUM	0.55617
MUGI	0.95746	Strumok-256	0.73563
MICKEY	0.57499	Strumok-512	0.86376

Table 12 – Results of the Serial Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.68433	Rabbit	0.34335
AES-256	0.54761	RC4	0.63467
Enocoro	0.54739	SALSA-20	0.52347
DECIM v2	0.44883	SNOW2.0-128	0.36832
GRAIN	0.35638	SNOW2.0-256	0.78322
HC -128	0.57221	SOSEMANUK	0.34567
HC -256	0.23488	TRIVIUM	0.67347
MUGI	0.34572	Strumok-256	0.72752
MICKEY	0.78763	Strumok-512	0.62366

Analyzing the value of P-value by the results of the Maurer's "Universal Statistical" Test (Table 10), one can say whether the sequence is too compressed. The greater the value of P-value, the less compresable is the sequence. As a result of the Linear Complexity Test (Table 11), it is possible to determine whether the linear shift register exists in the sequence generator. The higher the value of P-value – the larger the size of the shift generator is required to reconstruct the sequence.

For random sequences, this size is about half its length. For a small value of P-value for tests from Table 12, the heterogeneity of the sequence sub-blocks is implicitly indicated.

Table 13 – Results of the Approximate Entropy Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.27357	Rabbit	0.34791
AES-256	0.39911	RC4	0.34671
Enocoro	0.12951	SALSA-20	0.86884
DECIM v2	0.27339	SNOW2.0-128	0.10917
GRAIN	0.19162	SNOW2.0-256	0.79903
HC -128	0.33410	SOSEMANUK	0.61877
HC -256	0.07352	TRIVIUM	0.52246
MUGI	0.36244	Strumok-256	0.41764
MICKEY	0.09856	Strumok-512	0.31153

Table 14 – Results of the Cumulative Sums (Cusums) Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.42853	Rabbit	0.68396
AES-256	0.64328	RC4	0.53665
Enocoro	0.37563	SALSA-20	0.62532
DECIM v2	0.42514	SNOW2.0-128	0.47863
GRAIN	0.58636	SNOW2.0-256	0.54796
HC -128	0.68527	SOSEMANUK	0.44387
HC -256	0.47623	TRIVIUM	0.58935
MUGI	0.57836	Strumok-256	0.79836
MICKEY	0.36568	Strumok-512	0.59623

Table 15 – Results of the Random Excursions Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.67548	Rabbit	0.73477
AES-256	0.77585	RC4	0.34773
Enocoro	0.34648	SALSA-20	0.75442
DECIM v2	0.46672	SNOW2.0-128	0.83739
GRAIN	0.57847	SNOW2.0-256	0.63478
HC -128	0.34678	SOSEMANUK	0.42488
HC -256	0.87343	TRIVIUM	0.45547
MUGI	0.49898	Strumok-256	0.84743
MICKEY	0.73987	Strumok-512	0.62398

Table 16 – Results of the Random Excursions Variant Test

The name of the cipher	P-value	The name of the cipher	P-value
AES-128	0.59235	Rabbit	0.58363
AES-256	0.40247	RC4	0.35872
Enocoro	0.13462	SALSA-20	0.54290
DECIM v2	0.38366	SNOW2.0-128	0.68125
GRAIN	0.48532	SNOW2.0-256	0.47193
HC -128	0.59291	SOSEMANUK	0.74821
HC -256	0.48363	Strumok-256	0.68223
MUGI	0.59254	Strumok-512	0.51944
MICKEY	0.39660	TRIVIUM	0.39576

The greater the value of P-value by the result of the test for approximate entropy (Table 13), the greater the degree of uncertainty of the values in the sequence. The smaller the value of P-value in Table 14, the greater the excessive uniformity of the distribution of values over the sequence. If the value of P-value from table 15 is too small, then it means that there is a deviation of the distribution of the selected template in all sub-blocks of the sequence. Finally, for the Random Excursions Variant Test (Table 16): if the value of P-value is too small then it means that there is a deviation of the distribution of the selected template in all subsequences. Thus, as shown in tables 2-16, all researched cryptographic algorithms have good statistical properties. In particular, according to the criterion "P-value < 0,01" it is concluded that all the formed sequences are random, and the corresponding generators can be used for cryptographic purposes.

The results of experimental statistical studies generally coincide with published earlier data and conclusions for the studied stream ciphers Enocoro, Decim, Grain, HC, MUGI, Mickey, Rabbit, RC-4, Salsa 20, SNOW 2.0, Sosemanuk, Trivium [2-7] and block algorithm AES [14,15]. However, according to the results of the comparative analysis values of statistical safety, ciphers SNOW 2.0 and Salsa 20 should be marked as the best. In addition, experimental studies of the output sequences of the Ukrainian algorithm Strumok [8,11] showed that according to statistical properties it is not inferior to world-known cryptographic algorithms.

4 Conclusions

In this work, an independent statistical testing of the most well-known stream symmetric ciphers, standardized at the national and / or international level, or presented as winners of international search projects, has been conducted. Our researches were conducted on equal terms and with identical initial parameters for all the ciphers under study. To do this, we used our own software implementation of cryptographic algorithms and the NIST STS statistical test suite.

During the execution of 15 statistical tests of NIST STS, the randomness of the binary sequences of modern stream symmetric ciphers was determined. Presented estimates, as expected, confirmed the high levels of their statistical security. According to the results of this work, it can be said that modern cryptographic algorithms fully meet the requirements for randomness and, as a consequence, reliable. However, it's important to note that there are algorithms that have shown better results throughout all tests, that is: SNOW 2.0 and Salsa 20.

It should be noted that the algorithm Strumok gives quite acceptable results in comparison with world analogues. This indicates that the sequence generated by the Strumok stream algorithm is close to random, that is, it is safe to use for cryptographic purposes.

The prospects for further research include a detailed analysis of the ciphers for the possibility of performing cryptanalytic attacks. It is advisable to investigate the ability of the considered ciphers, including the Strumok algorithm, to function reliably under post-quantum conditions, the main problems and prospects of which are studied in various works, for example, in [16-24].

References

[1] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 2010. URL: https://dl.acm.org/citation.cfm?id=2206233

[2] Information technology. Security techniques. Encryption algorithms. Part 4: Stream ciphers. ISO/IEC 18033-4, 2011. URL: https://www.iso.org/standard/54532.html

[3] Information technology. Security techniques. Lightweight cryptography. Part 3: Stream ciphers. ISO/IEC 29192-3, 2012. URL: https://www.iso.org/standard/56426.html

[4] Pseudorandom Number Generator Enocoro.URL: http://www.cryptrec.go.jp

[5] Decim – A new Stream Cipher for Hardware applications. ECRYPT Stream Cipher Project Report 2005/004. URL: http://www.ecrypt.eu.org/

[6] Hongjun W., Preneel B. Cryptanalysis of Stream Cipher Decim. URL: http://www.ecrypt.eu.org/stream/

[7] The eSTREAM Project. URL: http://www.ecrypt.eu.org/

[8] Kuznetsov O., Lutsenko M., Ivanenko D. Strumok stream cipher: Specification and basic properties. 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T). Kharkiv, 2016, p. 59-62.

[9] Kuznetsov A., Kolovanova Y., Kuznetsova T. Periodic characteristics of output feedback encryption mode. 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). Kharkov, 2017. pp. 193-198.

[10] The research of modern stream ciphers / Gorbenko I., Kuznetsov A., Lutsenko M., Ivanenko D. 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). Kharkov, 2017. pp. 207-210.
[11] Strumok keystream generator / Gorbenko I. and etc. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2018. pp. 294-299.
[12] Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2/ Kuznetsov A., Gorbenko Y., Andrushkevych A. , Belozersev I. 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). Kharkov, 2017. pp. 203-206.
[13] Research of cross-platform stream symmetric ciphers implementation/ Kuznetsov A., Frolenko V., Eremin E., Zavgorodnia O. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Kyiv, 2018. pp. 300-305.
[14] FIPS–197: Advanced Encryption Standard (AES). National Institute of Standards and Technology, 2001. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[15] ISO/IEC 18033-3:2010. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. URL: https://www.iso.org/standard/54531.html
[16] Deutsch D., Jozsa R. Rapid solutions of problems by quantum computation. Proceedings of The Royal Society of London. A: Mathematical, Physical and Engineering Sciences.1992. Vol. 439, №1907. pp. 553-558.
[17] Bernstein D., Buchmann J. , Dahmen E. Post-Quantum Cryptography. Berlin-Heidleberg: Springer-Verlag, 2009. 245 p.
[18] Post-Quantum Crystography: A combination of Post-Quantum Cryptography and Steganography/ Gabriel A. J., Alese B. K., Adetunmbi A. O., Adewale O. S. 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013). London, 2013. pp. 449-452.
[19] Code-based public-key cryptosystems for the post-quantum period / Kuznetsov A., Svatovskij I., Kiyan N., Pushkar'ov A. 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). Kharkov, 2017. pp. 125-130.
[20] Towards post-quantum security for IoT endpoints with NTRU / Guillen O. M. and etc. Design, Automation & Test in Europe Conference & Exhibition (DATE). Lausanne, 2017. pp. 698–703.
[21] Code-based key encapsulation mechanisms for post-quantum standardization / Kuznetsov A. and etc. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Kyiv, 2018. pp. 276-281.
[22] Baldi M., Santini P., Cancellieri G. Post-quantum cryptography based on codes: State of the art and open challenges. AEIT International Annual Conference. Cagliari, 2017. pp. 1-6.
[23] Alam M. S. Secure M-commerce data using post quantum cryptography. 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). Chennai, 2017. pp. 649-654.
[24] Post-Quantum Diffie-Hellman and Symmetric Key Exchange Protocols / Xiangdong Li and etc. 2006 IEEE Information Assurance Workshop. NY: West Point, 2006. pp. 382-383.

Рецензент: Іван Горбенко, д.т.н., професор, академік Академії наук Прикладної Радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна.
E-mail: gorbenkoi@iit.kharkov.ua

Надійшло: Вересень 2018.

Автори:

Олексій Нарежний, к.т.н., доцент факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна.
E-mail: o.nariezhnii@karazin.ua

Егор Еремин, студент факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна.
E-mail: suvenick2@gmail.com

Владислав Фроленко, студент факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна.
E-mail: jadson27101@gmail.com

Кирилл Чернов, студент факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна.
E-mail: kirillfilippsky@gmail.com

Татьяна Кузнецова, студентка факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна.
E-mail: kuznetsova.tatiana17@gmail.com

Евгений Деменко, студент факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна.
E-mail: demenjay@gmail.com

Статистичні властивості сучасних потокових шифрів.

Анотація. В останні роки в Україні продовжуються численні дослідження поточних симетричних шифрів, основною метою яких є аргументація принципів створення нового криптографічного алгоритму, на основі якого може бути прийнято національний стандарт. Одним з найважливіших аспектів вибору з багатьох варіантів є статистичні властивості вихідної псевдовипадкової послідовності (потоку ключів). У даній роботі отримані результати порівняльних досліджень статистичних властивостей вихідних послідовностей, які формуються різними потоковими шифрами, зокрема, всесвітньо відомі алгоритми Enocoro, Decim, Grain, HC, MUGI, Mickey, Rabbit, RC-4, Salsa20, SNOW2.0, Sosemanuk, Trivium та український криптографічний алгоритм Струмок, розроблений в останні роки. Для порівняльних досліджень була використана методика NIST

STS, згідно з якою експериментальні дослідження виконуються в 15 статистичних тестах, метою яких є визначення випадковості вихідних послідовностей. Кожен з цих тестів спрямований на вивчення певних вразливостей генератора, тобто вказує на потенційне використання різних методів криптографічного аналізу. Незважаючи на те, що розглянуті поточні алгоритми шифрування були вже досліджені раніше, ми провели статистичну перевірку сгенерованих послідовностей при однакових умовах і з однаковими початковими параметрами, тобто наші результати дозволяють провести порівняльний аналіз шифрів. Оцінки, представлені у статті, як і очікувалося, підтвердили високі показники статистичної безпеки сучасних шифрів. Крім того, за результатами експериментальних досліджень було встановлено, що новий український поточний шифр Струмок не поступається кращим світовим алгоритмам за статистичними властивостями послідовностей.

Ключові слова: симетрична криптографія; потокові криптографічні алгоритми; гамма; криптоаналіз; статистичні випробування.

Рецензент: Иван Горбенко, д.т.н., профессор, академик Академии наук Прикладной Радиоэлектроники, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы 6, 61022, г. Харьков, Украина.
E-mail: gorbenkoi@iit.kharkov.ua

Поступила: Сентябрь 2018.

Авторы:

Алексей Нарежный, к.т.н., доцент факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: o.nariezhnii@karazin.ua

Егор Еремин, студент факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: suvenick2@gmail.com

Владислав Фроленко, студент факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: jadson27101@gmail.com

Кирилл Чернов, студент факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: kirillfilippsky@gmail.com

Татьяна Кузнецова, студентка факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: kuznetsova.tatiana17@gmail.com

Евгений Деменко, студент факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина.
E-mail: demenjay@gmail.com

Статистические свойства современных поточных шифров.

Аннотация. В последние годы в Украине продолжаются многочисленные исследования потоковых симметричных шифров, основной целью которых является аргументация принципов создания нового криптографического алгоритма, на котором может базироваться национальный стандарт. Одним из важнейших аспектов выбора из многих вариантов являются статистические свойства псевдослучайной последовательности (потока ключей). В данной работе получены результаты сравнительных исследований статистических свойств последовательностей, которые формируются различными потоковыми шифрами, в частности, рассмотрены всемирно известные алгоритмы Enocoro, Decim, Grain, HC, MUGI, Mickey, Rabbit, RC-4, Salsa20, SNOW2 .0, Sosemanuk, Trivium и украинский алгоритм Струмок, разработанный в последние годы. Для сравнительных исследований была использована методика NIST STS, согласно которой экспериментальные исследования выполняются по 15 статистическим тестам, целью которых является определение случайности последовательностей. Каждый из этих тестов направлен на изучение определенных уязвимостей генератора, то есть указывает на потенциальное использование различных методов криптографического анализа. Несмотря на то, что рассмотренные алгоритмы шифрования были уже исследованы ранее, мы провели статистическую проверку сгенерированных последовательностей при одинаковых условиях и с одинаковыми начальными параметрами, то есть наши результаты позволяют провести сравнительный анализ шифров. Оценки, представленные в статье, как и ожидалось, подтвердили высокие показатели статистической безопасности современных шифров. Кроме того, по результатам экспериментальных исследований было установлено, что новый украинский поточный шифр Струмок не уступает лучшим мировым алгоритмам по статистическим свойствам последовательностей.

Ключевые слова: симметричная криптография; потоковые криптографические алгоритмы; гамма; криптоанализ; статистические тесты.