computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific Journal of Computing

INVESTIGATIONS OF THE BASIC COMPONENT OF FCSR – GENERATOR

V.P. Shyrochin [1)], I.V. Vasyltsov [2)], B.Z. Karpinskij [2)]

1) Informatics and Computer Technique Department, National Technical University "Kyivsky Politechnichnyy Instytut", pr. Pobedy, 37, 03056, Kyiv, Ukraine,
E-mail: vpsh514@comsys.ntu-kpi.kiev.ua
2) Institute of Computer Informational Technology, Ternopil Academy of National Economy,
Lvivska 11, 46004 Ternopil, Ukraine, E-mail: iv@tanet.edu.te.ua, kbz@tane.edu.ua

Abstract: *The analysis of the statistical parameters of feedback with carry shift register (FCSR) quasi-random generator has been done. For the investigation were chosen 8 - bits and 9-bits registers. Were investigated the period of the generator and distribution of "one" and "zero" values. Additionally, the generated sequences where tested by NIST STS package.*

Keywords: - *Quasi Random Generator, LFSR, FCSR, stream cipher*

1. INTRODUCTION

Quasi-random generators (QRG) are widely used in different areas of national economy: Digital Signal Processing, Entertainment, Music and Graphics Composition, Simulation (including Artificial Intelligence) and Testing, Equation-Solving, Cryptography devices, etc [1].

There are different methods to develop QRG, but one of the most popular it is based on the shift register. Previously, the designers widely used linear feedback shift register (LFSR) as a basic component of such generators [2, 3]. But modern investigations in this area showed the perspective of the usage of feedback with carry shift register (FCSR) [3, 4].

Moreover, very promising is the mixed usage of both LFSR and FCSR as basic components to develop the QRG with high–resistant parameters [3]. On the Fig.1. the example of such usage it is shown.

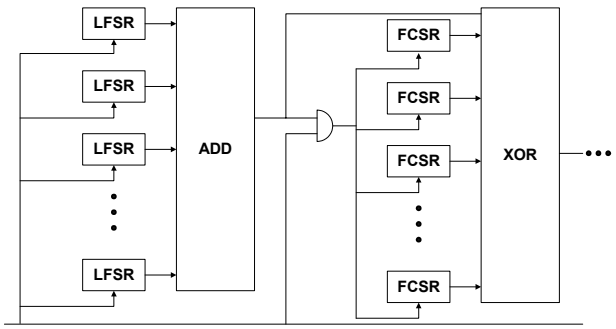

Fig.1 – Example of mixed usage of LFSR and FCSR components.

But FCSR component is relatively new, so there are few statistical investigations of it. That is why in this paper the authors show some results of statistical investigations of FCSR component. These will deep the theoretical basis of FCSR generators, and will allow developing new QRG structure.

2. FCSR COMPONENT

On the Fig.2 the Basic FCSR component has been shown.

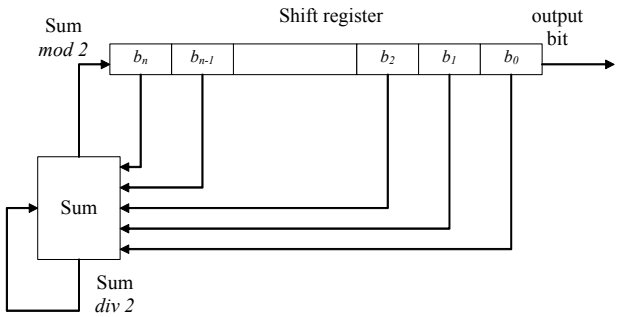

Fig.2 – Basic FCSR component.

The FCSR component is similar to LFSR constructively: both have shift register, and feedback function. The difference is in fact, that FCSR also has carry register. The FCSR component works in this way: feedback values are added to each other and to value of carry register. The obtained value *mod 2* is the generated bit, and obtained value *div 2* is the new value of carry register.

There are also next differences between LFSR and FCSR components:

1) carry register is not a bit, but a number. The size of carry register should be not less than $\log_2 t$, where t – the number of feedback lines;
2) during generation of quasi-random sequences it is the initial delay, before cyclic mode.
3) the maximal period of FCSR is defined as *q-1*, where q – determines the feedback links and can be defined as:

$$q = 2q_1 + 2^2 q_2 + 2^3 q_3 + ... + 2^n q_n - 1 \quad (1)$$

To obtain maximal period of sequence, q should be prime number, for which 2 is the primitive root (basic).

Any initial state of FCSR can be defined by certain shift register, feedback polynomial and the value of carry register. From this initial state FCSR can generate a sequence of maximal period after the initial delay, either generate the infinite sequence of '0' or '1' values, or can be a part of maximal period.

In the "open" literature [3, 4] there are relations, which allow obtaining the sequence of maximal period, generated by FCSR. But there is no information about the statistical parameters of the sequences, generated by such polynomials. Moreover, the considered polynomials are very sparse. So, investigations of FCSR component from this point of view are especially actual.

3. INVESTIGATION OF FCSR

Previously, [5, 6] the authors have done the statistical investigations of 8-bit LFSR component. Similarly, in this paper the statistical investigation of 8-bit and 9-bit FCSR components has been done.

On the Fig.3 the dependence of the sequence period, generated by certain 8–bit FCSR has been shown. Each FCSR was presented by the feedback polynomial in the decimal number equivalent area from 129 to 255. All polynomials has decimal number equivalent of odd numbers only. On the abscissa axis the ordinal number of polynomials has been shown, as well as on the axis of ordinates the obtained period of sequence has been shown.

The initial value of carry register was equal 0. The length of all sequences was equal 512 bits. But as it was discussed before some of the sequences have delayed before the cycle generating. This phenomena was taken into account, so showed results were obtained without delay value.

The maximal period was 508 bits. As it can be seen from the figure, there is the trend of increasing of the period value dependently on the value of feedback polynomial.

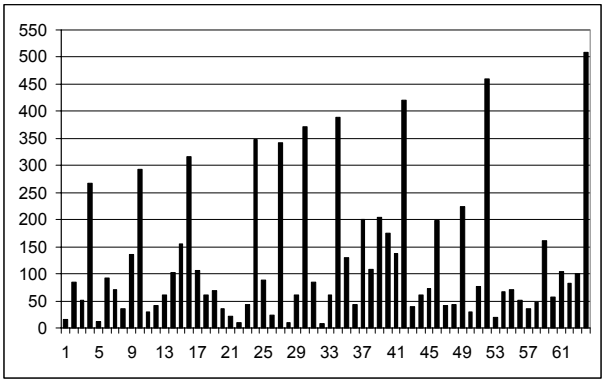

Fig.3 – Period of 8-bit FCSR accordingly to feedback polynomial.

On the Fig.4 the period of the 8-bit LFSR-generator, implemented on the different polynomials has been shown. These results were obtained from [5, 6] and allow comparing the result obtained in this article with result generated by equivalent 8-bit LFSR component.

Analysis of the Fig.3 and Fig.4 allows us to make two deductions, accordingly differences between LFSR and FCSR components:

1) the equivalent FCSR allow to obtain the sequence with potentially higher period;
2) the period of sequence, generated by FCSR component depends on the value of feedback polynomial.

Especially for the data protection task it is requested to investigate the uniformity of the distribution of the "zero" and "one" values. On the Fig.5 and Fig.6 the distribution of the "zero" and "one" values have been shown.

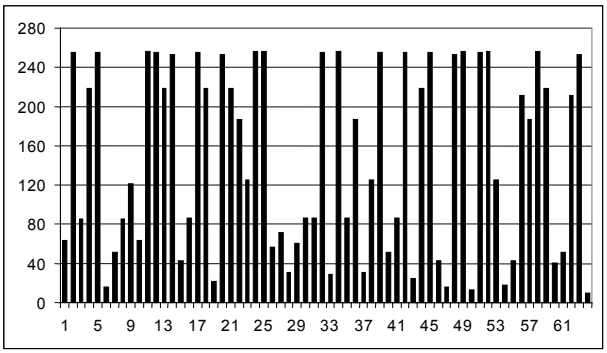

Fig.4 – Period of 8-bit FCSR accordingly to feedback polynomial.

As it can be see from the figures some anomalous results appeared. This phenomenon can be explained by the fact that some of the sequences has very short period, so the generated results are inapplicable to the data protection task.

Moreover, it was mentioned that "one" distribution has the bigger weight for the

polynomial. For the equivalent LFSR results [5, 6] one can see the inverse situation.

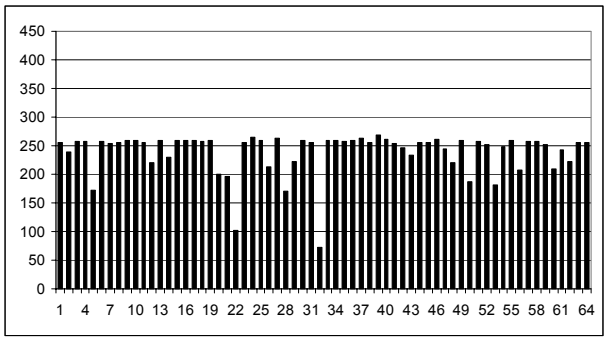

Fig.5 – The distribution of the "zero" values accordingly to feedback polynomial.

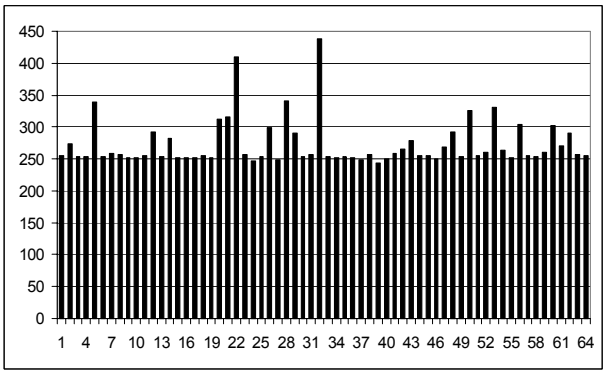

Fig.6 – The distribution of the "one" values accordingly to feedback polynomial.

On the Fig.7 – Fig.9 similar results, but for 9-bit FCSR component has been shown.

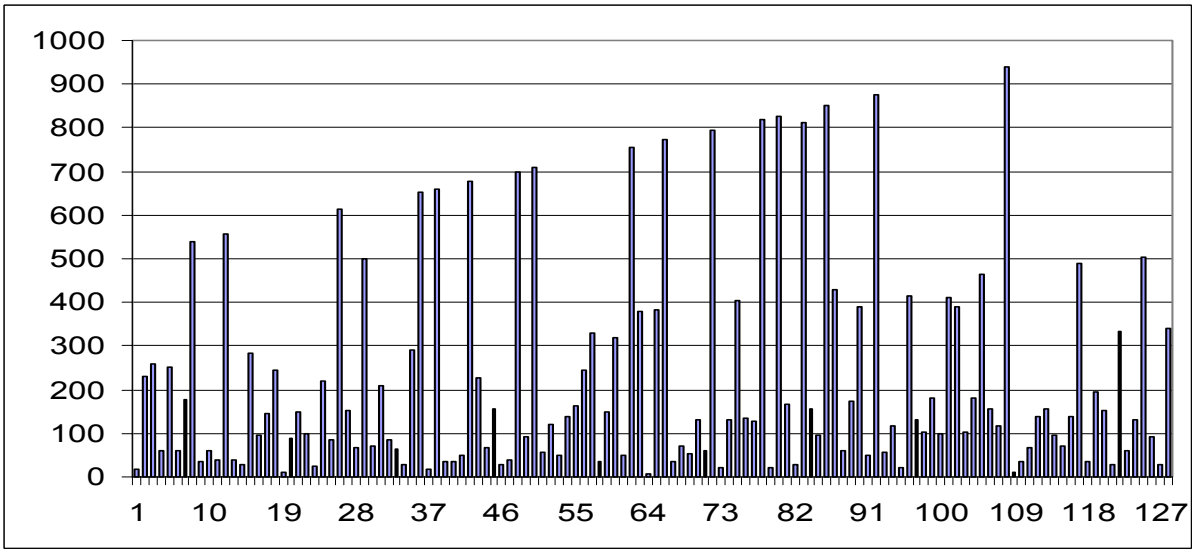

Fig.7 – Period of 9-bit FCSR accordingly to feedback polynomial.

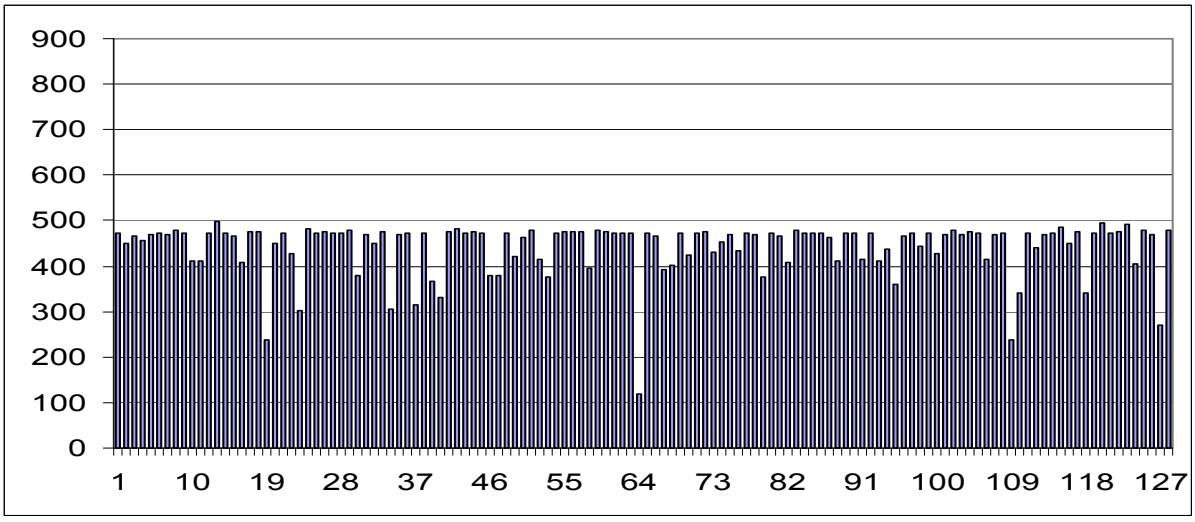

Fig.8 – The distribution of the "zero" values accordingly to feedback polynomial.

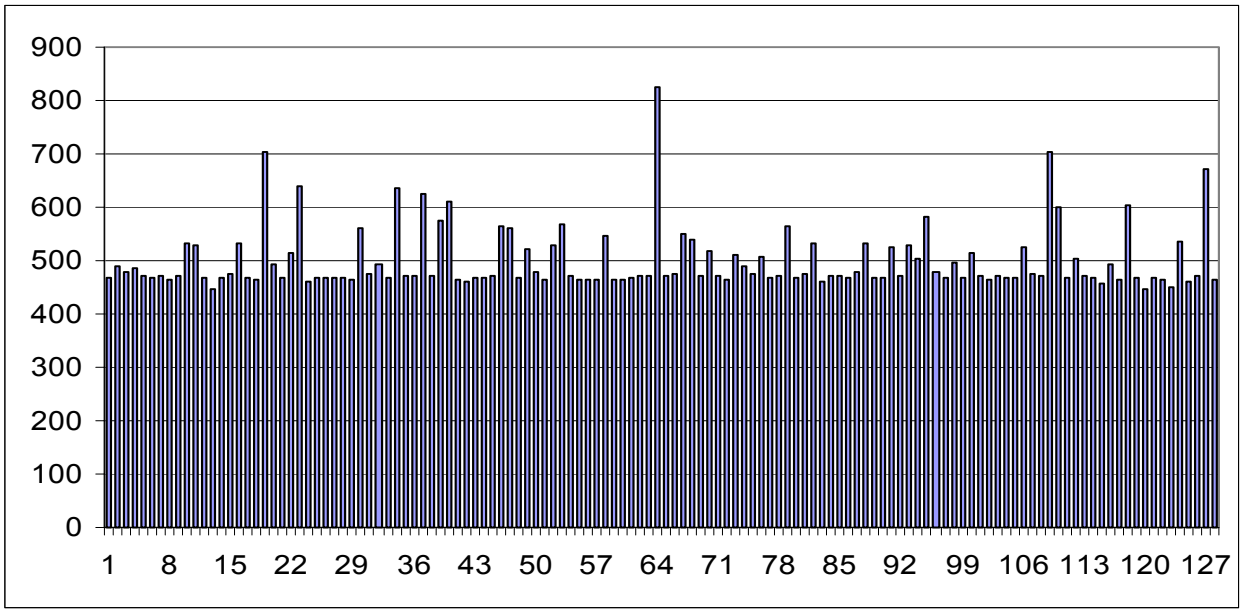

Fig.9 – The distribution of the "one" values accordingly to feedback polynomial.

Additionally some of the best results of 8-bit polynomials have been investigated by package NIST STS [7].

This is a special package designed by National Institute of Standardization and Technology (NIST) to test the sequences, generated by different QRG. The National Institute of Standards and Technology believes that these procedures are useful in detecting deviations of a binary sequence from randomness [7]. This package consists on 16 different statistical tests, which allow accepting (or rejecting) the hypothesis about randomness of the investigated sequence.

In our work only 3 tests were used, because other request at least the sequences of 100000 bit. There were Frequency Test, Runs Test and Cumulative Sums Test.

In the Table 1 and Fig.10-Fig.12 the results of testing of some of the obtained sequences has been shown.

The sequences, which has the period higher than 250, were tested. As it can be seen from the table and figures one of the tested sequences, generated by FCSR with feedback polynomial "11010011" has not passed all three tests. That mean, that it is necessary to reject hypothesis about uniformity of the distribution of the tested sequence. So, this polynomial should be avoided to use in the real world application for data protection system.

Table 1. Results of sequences testing by NIST STS package

#	Used polynomial	Test		
		Frequency	Runs	Cumulative sums
1.	10000111	0,0771	0,143794	0,006349
2.	10010011	0,111612	0,981176	0,061226
3.	10011111	0,063431	0,002692	0,115262
4.	10101111	0,002654	0,823121	0,003572
5.	10110101	0,595883	0,001115	0,003547
6.	10111011	0,426326	0,000256	0,110162
7.	11000011	0,859684	0,289443	0,004117
8.	11010011	0	0	0
9.	11100111	0,010369	0,000001	0,010428
10	11111111	0,027125	0,827531	0,019172

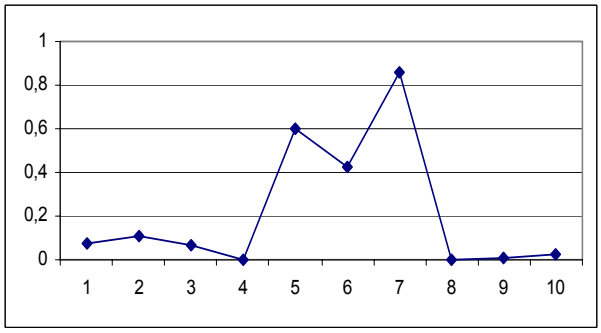

Fig. 10 – Results of sequences testing by Frequency test.

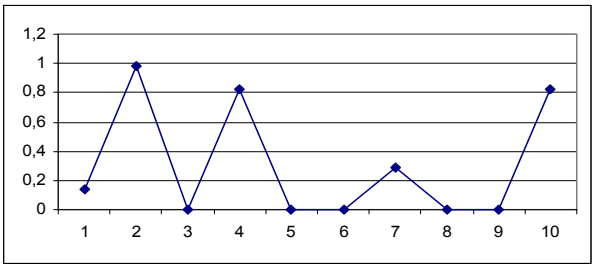

Fig. 11 – Results of sequences testing by Runs test.

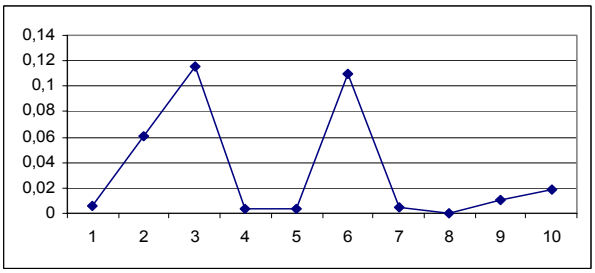

Fig. 12 – Results of sequences testing by Cumulative sums test.

4. CONCLUSION

In this paper the authors have investigated the statistical parameters of sequences, generated by FCSR component. The analysis showed that obtained sequences has higher period. But in the same time some of the sequences have not passed statistical tests. So for real world application it is advised to use the combination of LFSR and FCSR components to develop the advanced QRG.

5. REFERENCES

[1] D. Cambridge. Modern Methods and Applications of Random Number Generation in Signal Processing. In Proceedings of International Signal Processing Conference ISPC`2003, Dallas, TX, 31 March – 3 April 2003, ISBN # 1009129.

[2] K.Yu. Gundar, A.Yu. Gundar, D.A. Yanishevskiy. Information security in computer systems. K.: "Korniychuk", 2000. (in Russian).

[3] http://www.unix.kg/cgi-bin/document.pl?lang=rus& id=17.

[4] A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.

[5] I. Vasyltsov, B. Karpinskiy, A. Fedorov. Statistical characteristics researching of pseudo-randomize sequences generator build on shift-register, Scientific journal of National University "Lviv Polytechnic", Radio-technique and telecommunications, No. 443. Lviv, 2002. pp. 39-45. (in Ukrainian).

[6] I. Vasyltsov, B. Karpinskij, A. Fedorov. Investigation of the Statistical Parameters of the LFSR Quasy-Random Generator. Proceedings of the Integrational Conference TCSET'2002 "Modern problems of radio engineering, Telecomunications and computer science", 18-23 February 2002, pp. 168-169.

[7] http://cs-www.ncsl.nist.gov/rng/SP800-22b.pd.

Igor V. Vasiltsov *has graduated National University "Lvivska Polytechnika", Ukraine in 1993 by speciality "Radioengineering, Development and Technology of Radioelectronics". In March`1999 he supported his Ph.D. thesis in Development of CAD/CAM System at National University "Lvivska Polytechnika", Ukraine.*

He is the Vice-Head, Associated Professor of Security of the Informational Technology Department, Institute of Computer Informational Technology, Ternopil, Ukraine.

Research interests: Generally the main research interests area occupy development of the modern high-reliable complex system, implemented on VLSI. Below more detailed direction of it have been cited:

- *development of CAD/CAM systems for digital devices designing;*
- *development of high-reliable devices within VHDL-Core Technology;*
- *development of original approaches to increase the reliability level of designed system;*
- *development and simulation of mathematical models of electromagnetic internal noises in the chip;*
- *development of evolutionary algorithms for multi-objective optimization;*
- *development of specialized computer system implemented with the security devices;*
- *applied cryptology systems, implemented on VLSI devices.*

Shyrochin Valerij *was born 1939 year in t. Tulchin of Ukraine, doctor of technical sciences, professor of the computers engineering and computer science, works into National technical University of Ukraine "Kiev politechnical institute" from 1962 year.*

Area of scientific work: mathematical theory Petri-nets in tasks of design of safety Software of special computer systems, methods and programming means of computer imitation and simulation of complex systems, processors and algorithms digital signal processing, methods and krypton algorithms of information security in computer systems. In the field of scientific interests suggests and develops the conception and architecture of the emotionally and moral-oriented artificial intelligence, that is realized the processors and functions of men conscious, subconscious and superconscious. Graduated 8 candidates of technical sciences. Has more than 150 scientific and literary published works, including three monographs and twenty methodical manual - text lectures.