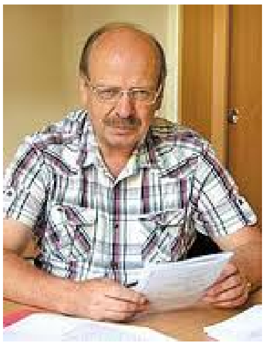
Generator of pseudorandom bit sequence with increased cryptographic security

M.M. Mandrona

post-graduate student, Ukraine, Lviv
Lviv Polytechnic National University
Lviv State University of Life Safety



V.M. Maksymovych

Doctor of Engineering Science, professor, Ukraine, Lviv,
Lviv Polytechnic National University

O.I. Harasymchuk

Ph.D. in Engineering Science, docent, Ukraine, Lviv,
Lviv Polytechnic National University

Yu.M. Kostiv

Ph.D. in Engineering Science, Ukraine, Lviv,
Lviv Polytechnic National University

Abstract
Generator of pseudorandom bit sequence with increased cryptographic security, at the basis of which there is an additive Fibonacci generator, is developed. Analytical expressions for speed and cryptographic security rating of the generator are given. The research results of statistic characteristics of output bit sequence with the help of NIST tests are given.

Key words: GENERATOR OF PSEUDORANDOM BIT SEQUENCE, CRYPTOGRAPHIC SECURITY, OPERATION SPEED, STATISTICAL CHARACTERISTICS.

In conditions of wide usage of computing technology and means of data exchange, there spread the possibilities of its leakage and unauthorized access with criminal purpose. It is necessary to chose reasonably the measures and support tools for data security to prevent crimes or decrease the damage from them. Among such means cryptographic means became a frequent practice, where generators of pseudorandom bit sequence (GPBS) are the integral part in most cases. They are particularly used for key generation, in stream ciphers, during formation of digital signature. GPBS are also frequently used in the sphere of technical information protection for depression of electromagnetic emission, noise pollution, during construction of noise signal generators, scrambler and they are components of protection in mobile communications. So the development of qualitative and reliable GPBS is considered to be one of the most important tasks of modern engineering and theoretical cryptography.

Today there exist a lot of ways of formation of pseudorandom sequences, developed great number of GPBS, which vary by their characteristics, where the main are: cryptographic security, statistical characteristics, operation speed and technologicalness in case of its hardware implementation.

The aim of this work is the development of generator of pseudorandom bit sequence, where on retention of high rates of technologicalness, productiveness and statistic characteristics, which are peculiar to modified additive Fibonacci generators (MAFG) [1-4], there achieved increase of the cryptographic security level.

In the previous work [5] MAFG and the ways for their improvement were considered in a detailed way. Generators of such type are not crypto secure as except initial installations of registers there are no another ways for its providing, which is obviously not sufficient. That is why we tried to increase crypto security of MAFG, having complicated its architecture, adding extra structural elements.

Figure 1 represents the structural scheme of GPBS on the base of MAFG with increased crypto secure and its simplified image with marked block of crypto security increase (BCSI) is shown in the figure 2.

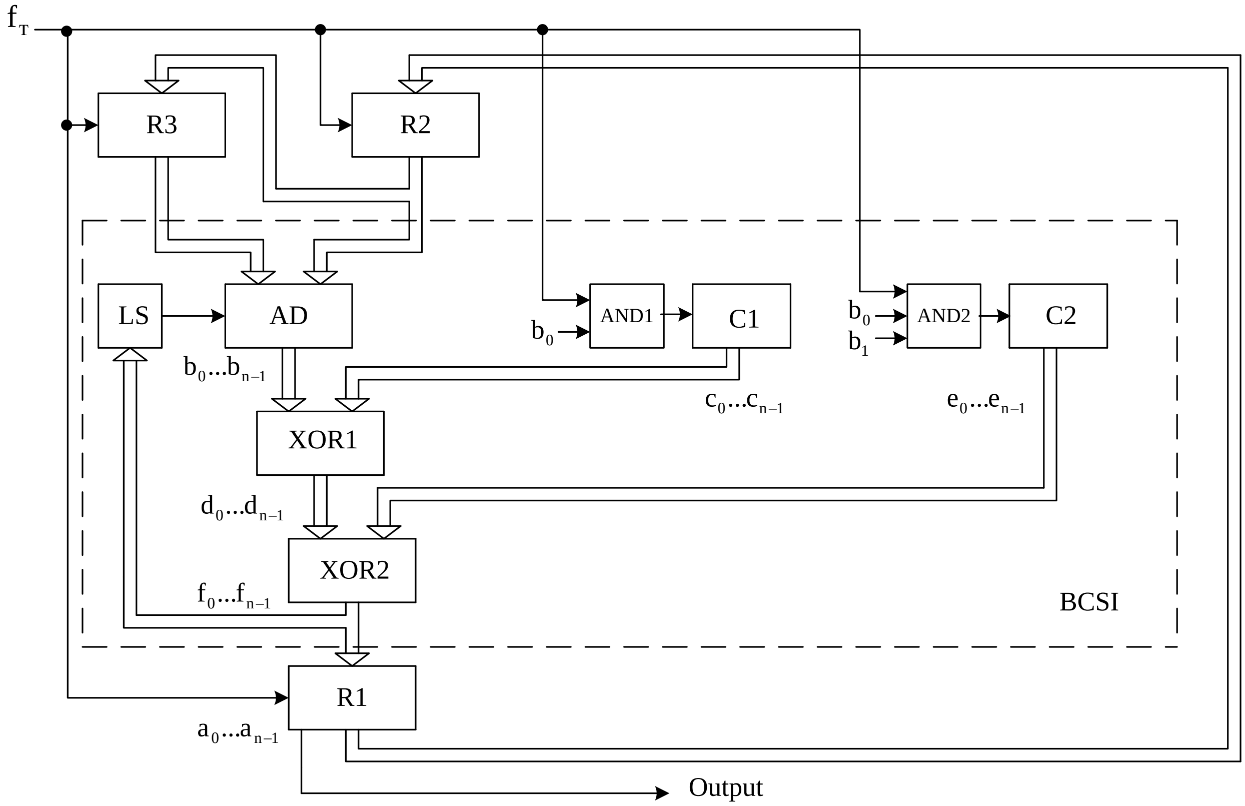


Figure 1. Structural scheme of GPBS on the base of MAFG

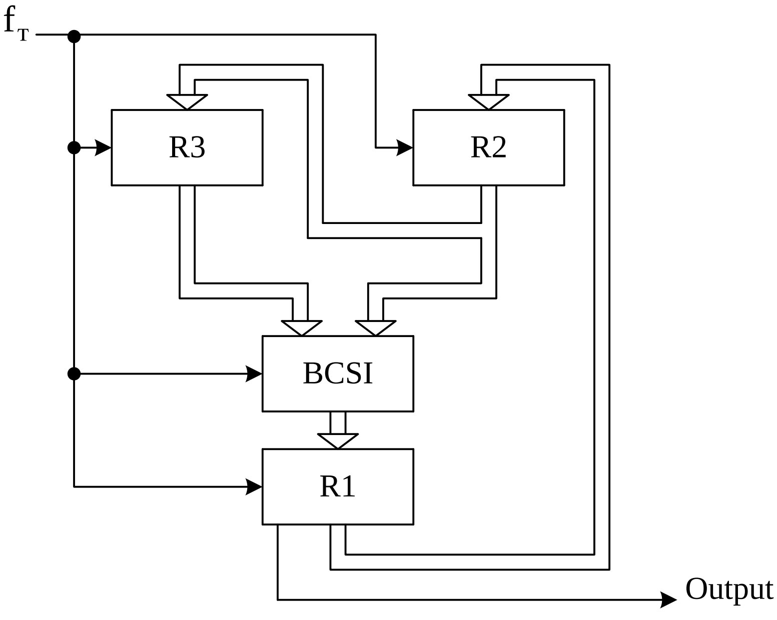


Figure 2. Simplified structural scheme of GPBS on the base of MAFG

Registers R1 – R3, coincidence adder AD, logic scheme LS, blocks of XOR logic elements XOR1 and XOR2, counters C1 and C2 and logic elements AND1 and AND2 are included into the generator. The work of generator is described by the following equations:

$$Q_1(t+1) = F(t),$$
$$Q_2(t+1) = Q_1(t), \quad (1)$$
$$Q_3(t+1) = Q_2(t),$$

where $Q_1(t)$, $Q_2(t)$, $Q_3(t)$ and $Q_1(t+1)$, $Q_2(t+1)$, $Q_3(t+1)$ - numbers in registers R1-R3 in the current and next cycles of device operation, $F(t)$ – is the number in the output of XOR 2 being formed in result of addition modulo 2 binary bits $d_0 \dots d_{n-1}$ of $D(t)$ number in the output of XOR 1 and binary bits $e_0 \dots e_{n-1}$ of $E(t)$ number in the output of C2:

$$F(t) = D(t) \oplus E(t) \qquad (2)$$

The number $D(t)$ is formed in result of addition modulo 2 binary bits $b_0 \dots b_{n-1}$ of $B(t)$ number in the output of AD and binary bits $c_0 \dots c_{n-1}$ of the number $C(t)$ in the output of C1:

$$D(t) = B(t) \oplus C(t) . \qquad (3)$$

$B(t)$ number is formed as follows:

$$B(t) = [Q_2(t) + Q_3(t) + a] \bmod 2^n \qquad (4)$$

where n – the number of structure elements bits.

Value of a variable *a* is determined by logical equation:

$$a = f_0 \oplus f_1 \oplus \dots \oplus f_{n-1} \qquad (5)$$

where $f_0 \dots f_{n-1}$ - the binary bits in the output of XOR2 (output of BCSI).

Clock pulses pass in input of C1 under the condition if $b_0 = 1$, in the input of C2 if $b_0 = b_1 = 1$. These conditions may vary and enter together with initial settings of C1 and C2 into the key, the length of which will determine the level of generator cryptographic security.

Output bit sequence is formed in the output of least significant bit of R1 register.

Operation speed of generator, considering that the counters work more slowly than the registers, may be estimated by the action time of scheme elements:

$$t = t_C + t_{AD} + t_{LS} + 2 \cdot t_{XOR} \qquad (6)$$

where t_C is the time of action of C1 and C2, t_{AD} - time of action of AD, t_{LS} - time of action of LS, t_{XOR} - time of action of XOR1 and XOR2 blocks.

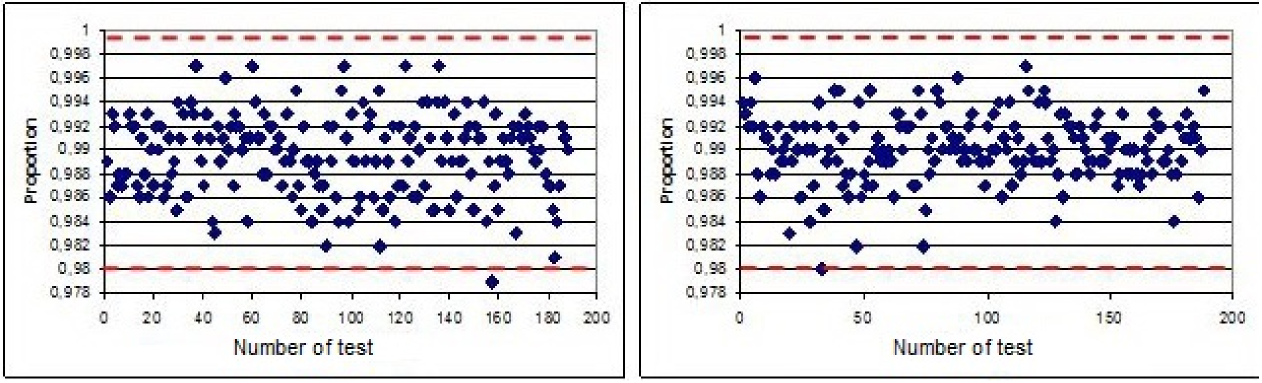
Crypto security of generator is determined by the amount of initial settings combinations choice of C1 and C2 and the amount of commutation choice of logic elements AND1 and AND2.

Total amount of such variants may be estimated by the expression:

$$K_1 = 2^n \cdot 2^n \cdot n \cdot n \cdot (n - 1) \qquad (7)$$

Considering that any bit positions of the number in the AD output may be fed on the control inputs of logic elements AND1 and AND2.

The figure 3 shows the results of analysis of statistic characteristics of output sequence of investigated generator at various separately chosen values of initial C1 and C2 conditions.



a b

Figure 3 Statistic images of GPBS with different initial values of counters: a- Counter 1=1, Counter 2=2; b- Counter 1=5, Counter 2=7

Along the axis of abscissa there put the number of NIST test, along the axis of the ordinates – is the probability of test pass. The test is considered to be passed when the probability of test pass is within the limits from 0.98 to 1.00, otherwise – the test is failed [6, 7]. Confidence limits are defined by dot line for clarity.

The table 1 represents detailed test results of output bit sequence of generator at various initial values of numbers in counters. So, statistic characteristics of GPBS do not depend on the initial conditions of C1 and C2.

Table 1 Test results of GPBS when changing the initial values of counters

Initial values of counter numbers		NIST test results	
Counter 1	Counter 2	Number of tests	
		Failed	Passed
1	2	1	187
5	7	0	188
23	33	1	187
171	393	1	187
393	171	0	188
1487	2111	0	188
14051	30211	0	188
171078	712731	0	188
23	30211	1	187
30211	23	0	188

Conclusions

Undertaken studies have confirmed the high quality of developed GPBS. Further improvement of its qualities is possible when: there are structure changes of basic MAFG due to increase of amount of registers storing of previous values of pseudorandom numbers, increase of amount of structural element bits, complication of BCSI operation.

References

1. Mascagni M. Parallel Pseudorandom Number Generation. Advanced architecture Computers. 1995, P. 42-48.
2. Anderson P. A Fibonacci-based pseudo-random number generator. Available at: http://link.springer.com/chapter/10.1007/978-94-011-3586-3_1#page-1
3. Orue A. B., Montoya F., L. Hernández Encinas. Trifork, a New Pseudorandom Number Generator Based on Fibonacci Maps. *Journal of computer science and engineering*, volume1, issuex, xxx 2010. Available at: http://iliasistemas.com/descargas/TRIFORK.pdf
4. Ivanov M.A., Chugunkov I.V. Kriptograficheskie metody zashchity informatsii v komp'yuternykh sistemakh i setyakh: uchebnoe posobie. Moscow, Izd-vo NIYaU MIFI, 2012, 400 p.
5. Kostiv Yu.M., Maksimovich V.M., Mandrona M.M., Garasimchuk O.I. (2013). Hardware implementation and investigation of modified Fibonacci generators. *Komp'yuterni tekhnologiï drukarstva. L'viv: Vid-vo Ukraïns'koï akademiï drukarstva.* No 29, p. 167-174.
6. Mandrona M.M., Maksimovich V.M., Kostiv Yu.M., Garasimchuk O.I. (2013). Investigation of the influence of generator Gollmann parameters on the statistic characteristics of signal output. *Visnik of Kremenchuk Mykhailo Ostrohradshyi National University*, Kremenchuk, KrNU. No 4 (81). P. 98-103.
7. Gorbenko I.D., Gorbenko Yu.I. Applied cryptology: Theory. Practice. Application: monography. Kharkiv, Fort, 2012, 880 p.