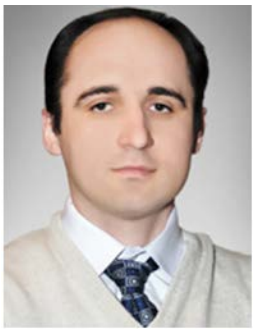
Development of a statistical security pseudorandom bit sequence generator by applying the systemic theoretical approach

Mandrona M.M.

Ph.D. in Engineering Science, senior lecturer, Ukraine, Lviv,
Lviv State University of Life Safety

Maksymovych V.M.

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



Harasymchuk O.I.

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

Kostiv Yu.M.

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

Abstract
A statistical security pseudorandom bit sequence generator has been developed on the basis of additive Fibonacci generator. Studies have been conducted into the quality of its operation according to the criteria of systemic theoretical approach to the design of generators. The said criteria include: pulse repetition period, statistical characteristics, linear complexity, key information amount (length of key) and clock rate.
Keywords: GENERATOR OF PSEUDORANDOM BIT SEQUENCE, A STATISTICAL SECURITY, ENSURING BLOCK OF STATISTICAL SECURITY, PROTECTION OF INFORMATION

Introduction

In the present-day world of information technologies, pseudorandom numbers are widely used in various areas of science and technology, in particular, in the data protection systems, in the latest telecommunication systems, in the measurement technology. In the area of data protection, pseudorandom numbers are being used for stream encryption of communication channels, generation of keys for cryptographic systems, information hashing (randomisation), creation of a digital signature, as well as in order to create different sort of noise masking etc. It has been ascertained that the characteristics of the security systems depend upon the characteristics of their cryptographic subsystems that are determined not only by the applied algorithms but also by the qualitative indicators of the applied pseudorandom sequences. Since the key is crucial to the issue of security of a cryptographic system, application of an unreliable process in the course of key generation shall render the entire cryptosystem vulnerable.

Development of generators is a process commenced a long time ago and there are lots of them; the crucial matter here is, however, the clock rate of such generators together with preservation of statistical safety. This is why, development of pseudorandom bit sequence generators that are not complicated as far as hardware is concerned and reliable at the same time increasingly becomes a pressing matter. Generators that are known to us at the present time have good clock rate and are simple in terms of hardware; they do not always, however, comply with the requirements pertaining to randomness whereas development of cryptologically stable generators usually causes losses in the clock rate and complication of their structure. All of the above parameters usually are in contradiction to each other.

The referenced studies [1, 2] state that there exist four different approaches to the development of stream ciphers that can also be fully applied in the course of development of PRBSGs, the inalienable integral part of the said ciphers; these approaches are, specifically: systemic theoretical approach; information theoretical approach; complexity theoretical approach; randomised approach.

Since the generators that are being examined in the present article are built on the basis of the element base (hardware components) of digital equipment, it is thereby natural to apply the systemic theoretical approach.

The purpose of the present study is to develop a statistical security pseudorandom bit sequence generator which would retain high degree of clock rate and simple hardware implementation at the same time.

Essential Part of the Study

As a basis for the PRBSG development, we have chosen the structure of the additive Fibonacci generator (AFG) since such devices are known to have a high clock rate but are also known to be unreliable as far as statistical characteristics are concerned [3].

In the referenced studies [4, 5], we have suggested a method which would allow to enhance the statistical characteristics of an AFG by way of supplementing its structure with an additional logical circuit. As a result of the study, we have managed to attain statistical security of a generator at a minimum number of bits – $n = 23$. There remains, however, the task to create a statistically security PRBSG which would retain a high clock rate and would be simple in terms of hardware at the same time.

In order to develop an AFG which would be characterised by enhanced statistical safety, the structure of a modified additive Fibonacci generator (MAFG) was used as a basis [4]. Thereby, in accordance with the systemic theoretical approach to the design process, the following rules were adhered to: each bit of the output stream must be a complex transformation of all or the majority of the key's bits; the redundancy in the structural elements should get dispersed and thus create a more blurred statistics.

The structure of the device is depicted in Figure 1. It contains registers ranging from R1 to R4, the

coincidence type adder AD, the logical circuit LC, the adder units 2, XOR 1 and XOR 2, the counters C1 and C2. Structural elements – AD, LC, XOR 1, XOR 2 and C1, C2 – may be compiled into a single unit which would be interpreted by us as the ensuring block of statistical security (EBSS).

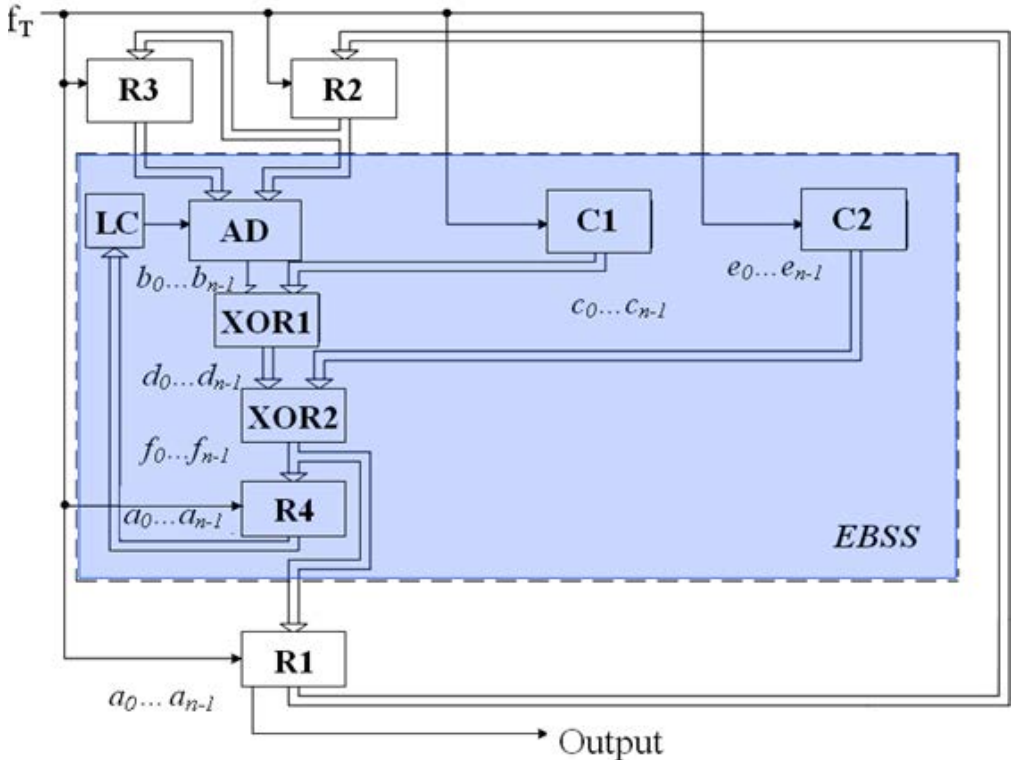


Figure 1. Structural scheme of GPBS on the base of MAFG with EBSS

A similar generator has already been examined by us in another referenced study [5]. The device that is being examined in the present work features some modifications that led to improvement of its statistical characteristics.

The work of generator is described by the following equations:

$$\begin{aligned} Q_1(t+1) &= F(t), \\ Q_2(t+1) &= Q_1(t), \\ Q_3(t+1) &= Q_2(t), \end{aligned} \qquad (1)$$

where $Q_1(t)$, $Q_2(t)$, $Q_3(t)$ i $Q_1(t+1)$, $Q_2(t+1)$, $Q_3(t+1)$ – number values 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 in modulus of 2 positions $d_0...d_{n-1}$ of $D(t)$ number in the output of XOR 1 and positions $e_0...e_{n-1}$ of $E(t)$ number in the output of $C2$:

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

The number $D(t)$ is formed by addition in modulus of 2 positions $b_0...b_{n-1}$ of $B(t)$ number in the output of AD and positions $c_0...c_{n-1}$ of the number $C(t)$ in the output of $C1$.

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

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

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

where n – the number of bit positions of structural elements of the scheme.

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

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

where $f_0...f_{n-1}$ – the value of bits in the output of XOR 2.

Researching of the Recurrence Period

The recurrence period of a PRBSG built on the basis of MAFG has been studied with the assistance of a simulation model. The period was recorded in those instances when there occurred a recurrence of the number values in the registers ranging from R1 to R3. The complexity of the study consists in the fact that the recurrence period must be ascertained for all possible combinations of seeds ('beginning numbers') values in the registers. If the number of binary bits of the device's structural elements is sufficiently high, this task is practically unfeasible due to the unacceptably long modelling time. For instance, if n=10, the complete enumeration shall require $2^{3n} = 2^{30} \approx 10^9$ time-steps. If the frequency of enumeration steps $f_{\text{п}} = 10^9$ Hz, the duration of complete study shall take 1 (one) second. If n=20, the complete enumera-

tion shall require $2^{3n} = 2^{60} \approx 10^{18}$ time-steps which, at the same frequency of enumeration, shall require 10^9 seconds which equates to approximately 32 years.

Keeping this in mind, it was decided to investigate the recurrence periods of the generator for smaller values of n, to determine certain existing conformities to law that might be extrapolated onto a large number of bits.

Figure 2 shows the results of the study into the recurrence periods of the generator – T_p for several values of *n*. Here

$$Q_0 = Q_{3\_0} + Q_{2\_0} \cdot 2^n + Q_{1\_0} \cdot 2^{2n} + Q_{4\_0} \cdot 2^{3n} + Q_{5\_0} \cdot 2^{4n}, \quad (6)$$

where Q_{1_0}, Q_{2_0} and Q_{3_0} stand for the seeds in R1, R2 and R3, whereas Q_{4_0} and Q_{5_0} stand for seeds in C2 and C1 respectively.

The stated results allow one to arrive at a conclusion that the recurrence period Tp is dependent upon the initial statuses of the generator structer elements, and that, as the number of bits, *n*, goes up, its maximum values also undergo a rapid increase and that more than a half of the Tp values are close to maximum values.

Detailed results of the study of recurrence period are stated in Table 1. Thereby, the modulus counter C1 equated to 2^n -1, whereas C2 2^n+1.

Researching of the Statistical Characteristics including Linear Complexity

Statistical characteristics have been researched with the application of the NIST tests which also include the reasearching of the linear complexity. The object of the tests was the bit sequence that is 10^9 bit long which was recorded from the least significant bit of the R1 register. The results of the tests are stated in Table 1. Thus, if $n \geq 13$, the formed bit sequence complies with the requirements pertaining to randomness whereas the generator that is forming such a sequence is statistical security.

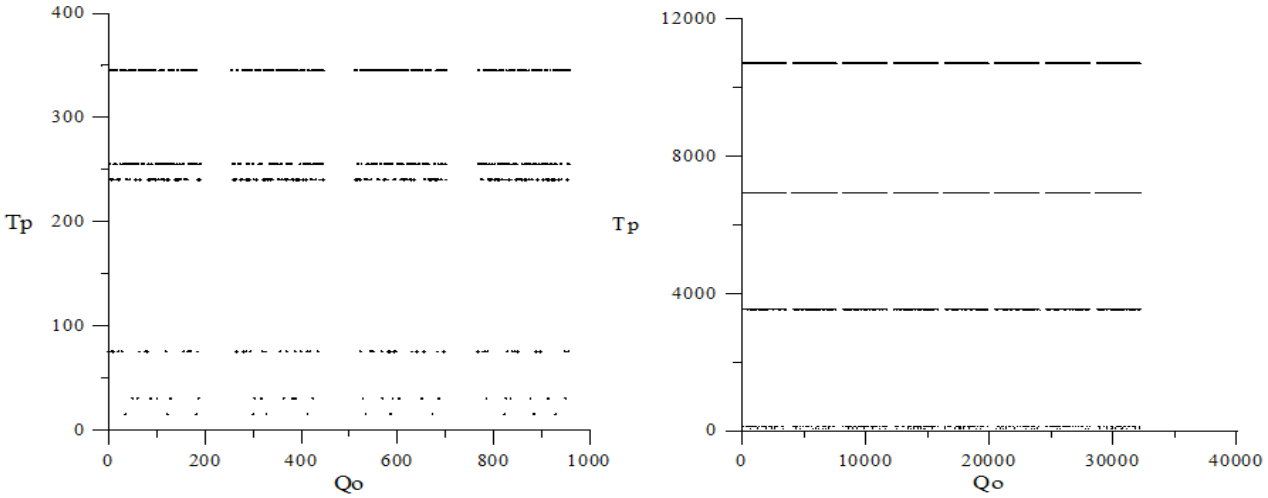


Figure 2. Dependence of the recurrence periods Tp from the initial statuses Q_0 of the R1 to R3 registers and the C1 and C2 counters: a) $n = 2$, b) $n = 3$

Determinating the Volume of Key Information (Key Length)

The following can be regarded as a cryptographic key of the generator: initial statuses of the registers ranging from R1 to R3 and the counters, C1 and C2. The complete set of values of these statuses equates to $Q_0^M = 2^{5n}$ at the key length being 5*n*. However, only a set that complies with the input bit sequences that have pass all of the NIST tests may be considered to be statistical security. If we consider the preceding studies, such a set includes at least $Q_0^C = 2^{5n-1}$ values, which corresponds to a key length of $5n$-1. In order to specify the Q_0^C set, we need to conduct additional studies.

Determinating of clock rate

Clock rate of a generator is determined by the maximum time that is required in order to complete the transition process in the circuit t_{ii} – a process that commences the moment when the operating front of the pulse reaches the clock input and completes with the formation of a new value of the number at the output of the coincidence type adder:

$$t_{nn} = t_C + t_{\text{AD}} + t_{LC} + 2 \cdot t_{\text{XOR}}, \quad (7)$$

where t_C – is the time of action of C1 and C2, t_{AD}– time of action of AD, t_{LC} – time of action of LC, t_{XOR} – time of action of XOR 1 and XOR 2 blocks.

The maximum possible frequency of clock pulses equates to:

$$f_{m_{\max}} = \frac{1}{t_{nn}} = \frac{1}{t_C + t_{LC} + t_{AD} + t_{XOR}} \quad (8)$$

Table 1. Results of the PRBSG study on the basis of MALFG with EBSS

Number of bits n	Set of values $Q_0^M = 2^{5n}$	Maximum value of the recurrence period		Test results (NIST tests)	Statistically reliable set $Q_0^C = 2^{5n-1}$
		$T_{p\,max}$	Conditions of determinating		
1	2^5	12	Sorting out $Q_{1\_0}, Q_{2\_0}, Q_{3\_0}, Q_{4\_0}, Q_{5\_0}$	-	–
2	2^{10}	345		-	–
3	2^{15}	10710		-	–
4	2^{20}	496485	$Q_{4\_0} = Q_{5\_0} = 0$, Sorting out $Q_{1\_0}, Q_{2\_0}, Q_{3\_0}$	-	–
5	2^{25}	27821508	$Q_{4\_0} = Q_{5\_0} = 0$, $Q_{1\_0} = 0$, $Q_{2\_0} = Q_{3\_0} = 1$	-	–
6	2^{30}	271891620		-	–
7	2^{35}	$> 10^9$		-	–
8	2^{40}	$> 10^9$		-	–
9	2^{45}	$> 10^9$		-	–
10	2^{50}	$> 10^9$		-	–
11	2^{55}	$> 10^9$		- 1	–
12	2^{60}	$> 10^9$		- 1	–
13	2^{65}	$> 10^9$		+	2^{64}
14	2^{70}	$> 10^9$		+	2^{69}

Thus, the clock rate of a generator primarily depends upon the response duration of AD and LC, since the registers of memory, R1 to R3, are operating simultaneously and any delay in their response duration equates to a delay in the duration of a response of one flip-flop.

The clock rate of the AD may increase if the known methods of building of coincidence type adders with parallel and serial parallel transfer are applied; in no way does this rate influence the period of repetition of a generator and its statistical characteristics.

The response duration of a logical circuit, LC depends upon the manner in which its circuit engineering is implemented as well as upon the number of the members of equation (5) which may be variable. A reduction of this number allows to substantially increasing the clock rate of the device as a whole. However, taking into account the fact that such a reduction may influence the recurrence period of the device and its statistical characteristics, it is necessary to conduct corresponding studies (determining the recurrence period and testing the compliance with statistical characterisics) – an undertaking that has been accomplished by us for certain instances of PRBSGs built on the basis of MAFG, as described in the referenced studies [4, 5].

Table 2 states technical characteristics of MAFG with EBSS obtained as a result of simulation with the assistance of the Foundation Series 4.1i automated designing system developed by Xilinx Company.

As one can see from the results of the study, the technical characteristics of the generator comply with the requirements pertaining to the PRBSG developers and may be practically used in various applied tasks, particularly in the tasks related to the information protection.

Table 2. Technical characteristics of PRBSG on the basis of MAFG with EBSS

Number of PRBSG bits	10
Number of coincidence type adder bits	8+2 (4)
Recurrence period of pseudorandom numbers	$>10^9$
Minimum period of clock pulses, nanoseconds	8.4
Maximum frequency of clock pulses, MHz	119.04

Conclusions

The studies that were conducted have verified the high quality of the PRBSG that was developed. The bit sequence formed already at $n \geq 13$ satisfies to the requirements of randomness – that is, the generator has statistical security. Its characteristics may be improved if: the basic MAFG is changed due to

increasing of registers number, if the number of structure elements bit and the number of generator's links are increased; as well as if the operation of the ensuring block of statistical security itself becomes more complex.

References

1. Rueppel R.A. "Stream Cipher", Contemporary Cryptology: The Science of Information Integrity, G.J. Simmons, ed., IEEE Press, 1992, p.p. 65-134.
2. Schneier B. Applied Cryptography. Protocols, algorithms, source code in C language. Moscow, Publishing House of the «Triumph», 2002, 797 p.
3. Ivanov M.A., Chugunkov I.V. Kriptograficheskie metody zashchity informatsii v komp'yuternykh sistemakh i setyakh: uchebnoe posobie [Cryptographic security methods of information in computer systems and networks. Study guide]. Moscow, NIYaU MIFI, 2012, 400 p.
4. Mandrona M.M., Maksymovych V.M. (2014). Investigation of the Statistical Characteristics of the Modified Fibonacci Generators. *Journal of Automation and Information Sciences.* 10.1615/J AutomatInfScien.v46.i12.60. p. p. 48-53.
5. Mandrona M.M., Kostiv Yu.M., Maksymovych V.M., Harasymchuk O.I. (2014). Generator of pseudorandom bit sequence with increased cryptographic security. *Metallurgical and Mining Industry.* No 5, p.p. 81-86.