Development of a statistically reliable pseudorandom bit sequence

Maria Mandrona[1], Volodymyr Maksymovych[2], Yuriy Kostiv[2], Oleh Harasymchuk[3]

[1]Department of Information Security Management,
Lviv State University of Life Safety, UKRAINE, Lviv,
Kleparivska street 35. E-mail: mandrona27@gmail.com

[2]Security of Information Technologies Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: yura.kostiv@gmail.com

[3]Academic Chair of Data Protection,
Lviv Polytechnic National University, UKRAINE, Lviv,
S. Bandery street 12, E-mail: garasymchuk@ukr.net

***Abstract* – A statistically reliable pseudorandom bit sequence generator has been developed on the basis of additive lagged Fibonacci generator. Studies have been conducted into its 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 rate of response.**

Key words – pseudorandom generator, protection of information, pseudorandom numbers, ensuring block of statistical security, statistic characteristics.

I. Introduction

In the present-day world of information technologies, pseudorandom numbers are widely used in various realms of science and technology, in particular, in the data protection systems, in the latest telecommunication systems, in the measurement technology. In the realm 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 miscellaneous 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 applied 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 [1, 2].

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

II. Results and Discussion

As a basis for the PRBSG development, we have chosen the structure of the additive lagged Fibonacci generator (ALFG) since such devices are known to have a high rate of response but are also known to be unreliable as far as statistical characteristics are concerned [1].

In the referenced studies [3, 4], we have suggested a method which would allow to enhance the statistical characteristics of an ALFG by way of supplementing its structure with an additional logical circuit. As a result of the study, we have managed to attain statistical reliability of a generator at a minimum number of digits, $n = 23$. There remains, however, the task to create a statistically reliable PRBSG which would retain a high rate of response and would be simple in terms of hardware at the same time.

In order to develop an ALFG which would be characterised by enhanced statistical safety, the structure of a modified additive lagged Fibonacci generator (MALFG) 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 input 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 Reg1 to Reg 4, the coincidence type adder AD, the logical scheme LS, the adder units 2, XOR 1 and XOR 2, the counters C1 and C2. Structural elements – AD, LS, 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).

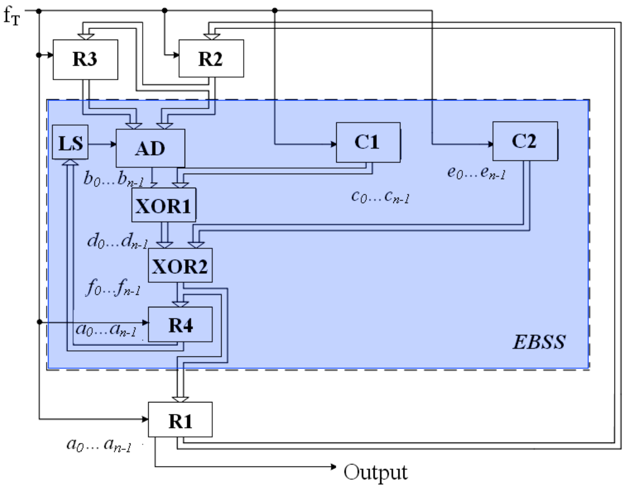

Fig. 1. Structural scheme of GPBS on the base of MAFG with EBSS

The following can be regarded as a cryptographic key of the generator: initial statuses of the registers ranging from Рг1 to Рг3 and the counters, Лч1 and Лч2. The complete set of values (magnitudes) of these statuses equates to $Q_0^M = 2^{5n}$ at the key length being 5n. However, only a set that complies with the input bit sequences that have pass all of the NIST tests may be considered to be statistically reliable. 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.

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 $Q_0^C = 2^{5n-1}$
1	2^5	12	-	–
2	2^{10}	345	-	–
3	2^{15}	10710	-	–
4	2^{20}	496485	-	–
5	2^{25}	27821508	-	–
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}

Statistical characteristics have been investigated with the application of the NIST tests [5] which also include the ascertaining 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 Pr1 register. The results of the tests are stated in Table 1. Thus, at $n \geq 13$, the formed bit sequence complies with the requirements pertaining to randomness whereas the generator that is forming such a sequence is statistically reliabl.

Response rate of a generator is determined by the maximum time that is required in order to complete the transition process in the t_{rp} circuit – 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:

$$t_{rp} = t_C + t_{AD} + t_{LS} + 2 \cdot t_{XOR} \ , \qquad (1)$$

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 XOR 1 and XOR 2 blocks.

The maximum possible frequency of timed pulses equates to:

$$f_{m_{\max}} = \frac{1}{t_{rp}} \ . \qquad (2)$$

Thus, the response rate of a generator primarily depends upon the response duration of AD and LS, since the registers of memory, Pr1 to Pr3, are operating simultaneously and any delay in their response duration equates to a delay in the duration of a response of one trigger.

Conclusion

The studies that were conducted have verified the high quality of the PRBSG that was developed. The bit sequence formed already at $n \geq 13$ complies with the the bit sequence complies with the requirements of randomness – that is, the generator is statistically reliable. Its characteristics may be improved if: the basic MALFG is changed at the expense of the increase of the number of registers, if the number of registers of structural elements and the number of generator's links is changed; as well as if the operation of the ensuring block of statistical security itself becomes more complex.

References

[1] M. A. Ivanov and I. V. Chugunkov Ed., "Teorija, primenenie i ocenka kachestva generatorov psevdosluchajnyh posledovatel'nostej [Theory, application, and quality assessnent of pseudorandom sequence generators]. Moscow: KUDITS-OBRAZ Publ., 2012.

[2] I. D. Horbenko and Iu. I. Horbenko Ed., Prykladna kryptolohiia: Teoriia. Praktyka. Zastosuvannia: monohrafiia [Applied cryptology: Theory. Practice. Application: a monograph]. – Kharkiv: Publishing House «Fort», 2012.

[3] M. M. Mandrona, V. M. Maksymovych "Investigation of the Statistical Characteristics of the Modified Fibonacci Generators" Journal of Automation and Information Sciences. 10.1615/J AutomatInf Scien.v46.i12.60, Pp. 48-53, 2014.

[4] M. M. Mandrona , Yu. M. Kostiv, V. M. Maksymovych, O. I. Harasymchuk, "Generator of pseudorandom bit sequence with increased cryptographic security", Metallurgical and Mining Industry. No 5, Pp. 81-86, 2014.

[5] NIST SP 800-22. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", csrc.nist.gov. [Online]. Available:http://csrc.nist.gov/publications/nistpubs//SP800-22rev1a.pdf [Accessed: April. 2010].