Implementation of modified additive lagged Fibonacci generator

Mandrona M.M.[1], Maksymovych V.M., Harasymchuk O.I.[2], Kostiv Yu.M.[3]

[1] Lviv State University of Life Safety, Department of Information Security Menegment
Kleparivska street 35, Lviv, Ukraine, e-mail: mandrona27@gmail.com
[2] Lviv Polytechnic National University, Department of the Information Security
S. Bandery street 12, Lviv, Ukraine, oleh.harasymchuk@gmail.com
[3] Lviv Polytechnic National University, Department of Security of Information Technologies
S. Bandery street 12, Lviv, Ukraine, e-mail: yura.kostiv@gmail.com

Generator of pseudorandom bit sequence with increased cryptographic security, which is based on additive lagged Fibonacci generator, is developed. The generator structure circuit and it work principle are described in the paper. There are also given two variants of it construction that are formed on programmable logic device developed by Xilinx company. The main generator characteristics are researched, in particular: recurrence period, fast-acting, statistical characteristics. In relation to the last the statistical portrait is presented, that was built with the help of NIST tests.

Keywords: generator of pseudorandom bit sequence, additive lagged Fibonacci generator, cryptographic security, operation speed, statistical characteristics

Introduction

Development of means of data protection as well as computing and measurement equipment has widened the realm of application of random and pseudorandom sequence generators.

Development of a pseudorandom sequence generator (PRSG) that is reliable and of proper quality is considered to be one of the paramount tasks of the present day applied theoretical cryptography [1,2]. The PRSGs are widely used for generation of keys and are the components of cryptographic systems, digital signatures, ensure other random parameters of cryptographic systems; they are also being widely used in the realm of technical protection of data in order to suppress the electromagnetic emissions, noise contamination in the premises, as well as in the course of building noise generators, scramblers, and are components of the mobile communication protection systems [3, 4].

Despite the fact that substantial developments have been made in the realm of design and implementation of such generators, a lot of unsolved issues remain that necessitate the search for new algorithms of operation, new approaches to design, optimisation of the structures of existing PRSGs, and improvement of their characteristics.

The study [5] focused upon the investigation of additive lagged Fibonacci generators with a delay. The main advantage of such generators as compared to other types of pseudorandom generator systems is their high response rate. Their statistical characteristics, however, are unsatisfactory – and so is, hence, also their statistical reliability. We have suggested a structure of a modified lagged Fibonacci generator with enhanced statistical characteristics [5, 7, 8].

The goal of the present article is to investigate the technical characteristics of a modified additive Fibonacci generator with a delay that is using Xilinx computer-assisted design (CAD) system.

Materials and methods

The modified additive lagged Fibonacci generator (MALFG) (see Figure 1) is comprised of a coincidence type adder 1, logical circuit 3, and memory registers 2_0, 2_1,…, 2_p, 2_{p+1},…, 2_q.

An MALFG operates in such manner that with every timed pulse in the registers ranging 2_0, 2_1,…, 2_p, 2_{p+1},… , 2_q new values (magnitudes) of numbers are being formed. In the 2_0 register, the number that is being determined by the input signal of the coincidence type adder 1, whereas in the registers ranging 2_j (j = 1, 2,…, q), numbers that are being determined by the input signals in the registers 2_{j-1}.

Timed pulse is necessary for the operation of a digital device, in this case, MALFG. With each timed pulse in registers 2_0,…, 2_q formed new value numbers.

At the output of the logical circuit 3, a signal is formed in accordance with the logical equation:

$$a = b_0 \oplus b_1 \oplus ... \oplus b_s , \qquad (1)$$

where b_k (k = 0, 1,…, S) stand for the values of binary bits of the number in the register 2_0, whereas S may obtain values ranging from 0 to m-1, where m stands for the number

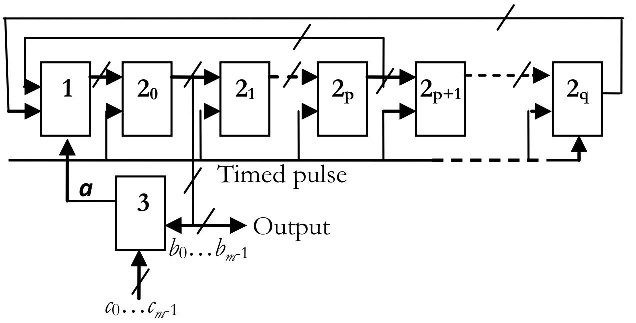

Figure 1. Structural scheme of a modified additive lagged Fibonacci generator: 1 – coincidence adder, 2 – registers, 3 – logical circuit

of binary bits of each of the registers ranging 2_0, 2_1,…, 2_p, 2_{p+1},…, 2_q. Therefore, in the course of operation of the logical circuit 3, any number of binary bits of register 2_0 may be engaged, as determined by the value of the code c_0,…, c_{m-1} at the control inputs of the generator.

As the next timed pulse arrives at 2_0 register, the number that is formed at the outputs of the coincidence type adder 1 is being recorded, in accordance with the expression

$$Q_i = (Q_{i-p} + Q_{i-q} + a) \bmod 2^m , \qquad (2)$$

where Q_i, Q_{i-p} and Q_{i-q} stand for the numbers in the memory registers 2_0, 2_p, and 2_q respectively.

Enhancement of statistical characteristics and an increase in the recurrence period of the proposed generator are confirmed by the results of the simulation described in the referenced study [5-8]. The study was conducted with a change in the number of the device's registers and the change of the number of their binary bits.

A simulation was conducted using the Foundation Series 4.1i CAD system developed by Xilinx company and an assessment was made of the basic technical characteristics of the MALFG operating in accordance with the following expression

$$Q_i = (Q_{i-3} + Q_{i-8} + a) \bmod 2^{10} \qquad (3)$$

The basic configuration of the MALFG circuit is depicted on Figure 2.

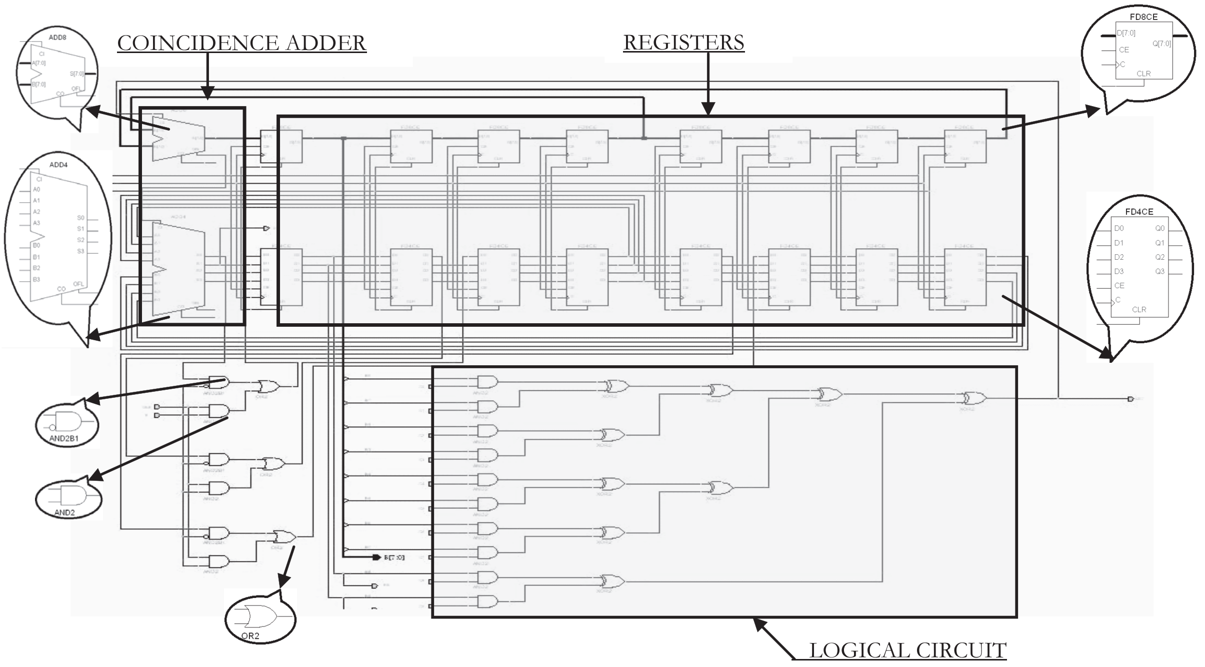

Figure 2. Basic configuration of a modified additive lagged Fibonacci generator (logical circuit – option 1)

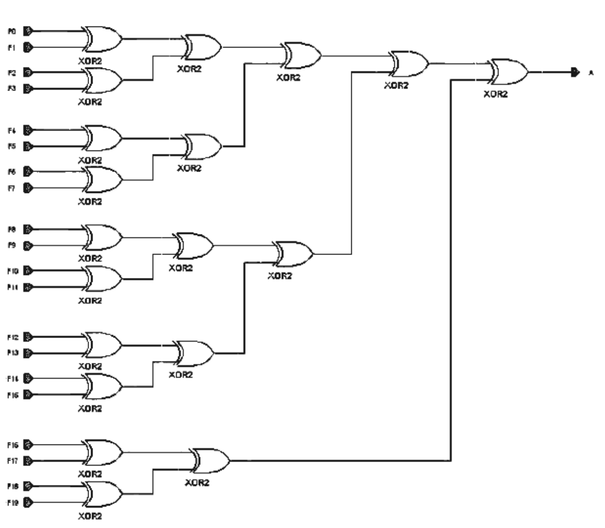

Figure 3. Logical circuit – option 2

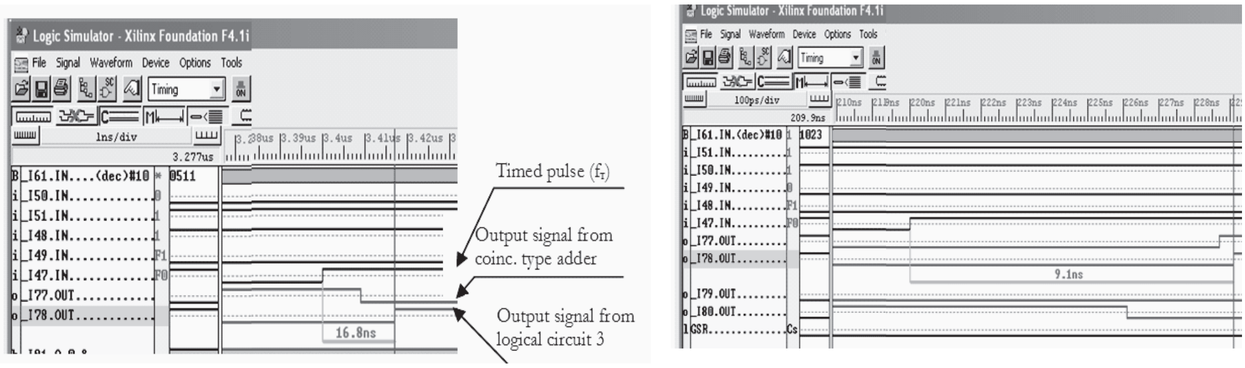

Figure 4. Results of the MALFG simulation using the Xilinx CAD system: a – option 1 of the logical circuit; b – option 2 of the logical circuit

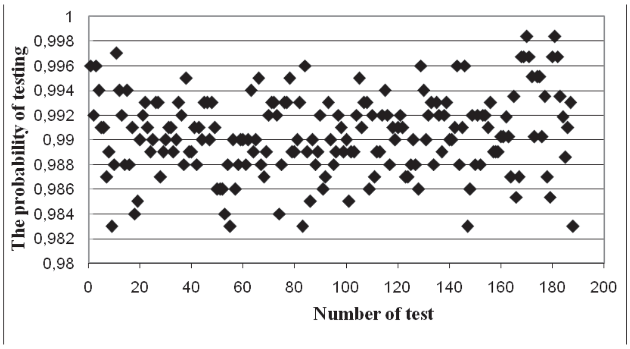

Figure 5. Statistical portrait of MALFG

Table 1. Basic technical characteristics

Technical characteristics	Value	
Number of MALFG bits	10	
Number of coincidence type adder bits	10	
Recurrence period of pseudorandom numbers	>109	
Modification of the logical circuit	Option 1	Option 2
Minimum period of timed pulses	16.8 ns	9.1 ns
Maximum frequency of timed pulses	29.76 MHz	54.95 MHz

The studies have been conducted with various options of a logical circuit – option 1 at Figure 2, option 2 at Figure 3.Figure 2 principle scheme represents structural PLD scheme implementation introduced on Figure 1.

Two LC variants, mentioned on Figure 2 and 3 are differ in speed and construction simplicity. Second variant is faster, but more complicated according high bits number. Choosing one of these variants depends on the requirements regarding common generator characteristics.

Results and discussion

Using the time interval analyser that is included in the CAD system package, an analysis was conducted of the time interval characteristics MALFG programmable logic device (PLD). In order to accomplish this, initially, using the Implementation option, optimal situation of the elements inside the PLD was arranged and the tracking of connections between them. The results of the MALFG modelling are shown on Figure 4, whereas the technical characteristics are provided in Table 1.

The minimum allowable duration of timed pulses was determined according to the maximum time required to complete the transition processes in the generator – that is, according to the timed interval between the front of the timed pulse and the front of the signal at the output of the LC logical circuit (see Figure 4).

If we take a look at the results of the MALFG modelling, we can observe an almost 50% decrease of the minimum duration of timed pulses caused by the application of a logical circuit from option 2 which, accordingly, increases the maximum frequency of timed pulses to a substantial degree. Assessment of the MALFG quality has been conducted using a set of NIST statistical tests. The object of the assessment was a sequence with a length of 10^9 bits that is being formed at the output of the least significant bit of the 2_0 register. The result of the test is shown at Figure 5 in the form of a statistical portrait.

As one may observe upon having examined the statistical portrait, all of the test values are within the 0.9805 – 0.9994 confidence range [6, 9] which testifies to the fact that the MALFG possesses satisfactory statistical characteristics. Thus, it may be concluded that the formed sequence is satisfied to the requirements pertaining to randomness.

Conclusions

The obtained results of technical characteristics as well as the results of the statistical assessment of the MALFG satisfied to the requirements to which the PRSG developers are subject and the said results may be applied in practice in the applied tasks.

Bibliography

[1] Gorbenko I.D., Gorbenko Yu. L. *Applied cryptology: Theory. Practice. Application: monography.* Kharkiv, Fort, 2012, 880 p.

[2] Ivanov M. A., Chugunkov I. V. *Kriptograficheskie metody zashchity informatsii v komp'yuternykh sistemakh i setyakh: uchebnoe posobie.* Moscow, 2012, 400 p.

[3] Anderson P.A., *Fibonacci-based pseudo-random number generator* [web page] http://link.springer.com/ chapter/10.1007/978-94-011-3586-31/[Accessed on 31 Sep. 2013.].

[4] Orue A. B., Montoya F., L. *Hernández Encinas: Trifork, a New Pseudorandom Number Generator Based on Fibonacci Maps*, Journal of computer science and engineering, Vo 1, issuex, xxx 2010, [web page] http://iliasistemas.com/descargas/TRIFORK.pdf/ [Accessed on 31 Sep. 2015.].

[5] Mandrona M.M., Maksimovich V.M., Kostiv Yu.M., Harasymchuk O.I., *Modification Fibonacci generator, Journal of current information protection*, Vo 2, pp. 56-62, May 2014.

[6] Mandrona M.M., Maksimovich V. M., Kostiv Yu. M., Harasymchuk O.I., *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), pp. 98-103, 2013.

[7] Mandrona M.M., Maksymovych V. M., *Investigation of the Statistical Characteristics of the Modified Fibonacci Generators,* Journal of Automation and Information Sciences/J AutomatInfScien.v46.i12.60, pp. 48-53, Dec. 2014

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

[9] NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. April, 2010.

Author(s):

PhD Mariia MANDRONA, *Senior lecturer of Information Security Menegment Department of Lviv State University of Life Safety.*

Dr. Sc. Professor Volodimir MAKSYMOVYCH, *Head of the Information Technology Security Department of Lviv Polytechnic National University.*

PhD Yuriy KOSTIV *– Assistant Professor of the Information Technology Security Department of Lviv Polytechnic National University.*

PhD Oleh HARASYMCHUK *– Assistant Professor of the Information Security Department of Lviv Polytechnic National University.*

Received: 7 October 2015
Received in revised form: 23 March 2016
Acepted: 24 March 2016