Additive Fibonacci Generators Using Prime Numbers

Volodymyr Maksymovych[1], Oleh Harasymchuk[2], Mariia Mandrona[1,3]

1. Department of Information Technology Security, National University "Lviv Polytechnic", Ukraine, Lviv, 12 Bandera street E-mail: volodymyr.maksymovych@gmail.com
2. Department of Information Security, Lviv Polytechnic National University, Ukraine, Lviv, 12 Bandera street, E-mail: oleh.harasymchuk@gmail.com,
3) Department of Information Security Management, Lviv State University of Life Safety, Ukraine , Lviv, 35, Kleparivska street., mandrona27@gmail.com

Abstract - The researching of additive Fibonacci generators is carry out in the work. The realization of generators differs from the traditional ones thanks to the use of prime numbes, which provides the constancy of the output pulse sequence repetition period in the whole range of possible values of initial settings − keys

Key words - information security, generators of pseudorandom sequences, prime numbers, additive Fibonacci generator, statistical characteristics.

I. Introduction

Additive Fibonacci Generators (AFG) are widely used in information security devices to form pseudorandom sequences of numbers or bits. By themselves, they are notcryptografhically secure but on their basis can be created quite safe for cryptanalysis generators [1].

The algorithm of classical AFG is formed on the basis of equation:

$$x_i = (x_{i-l} + x_{i-k}) \bmod(m), \quad (1)$$

where $l > k > 0$, or in a more general form

$$x_i = (x_{i-a} + x_{i-b} + ... + x_{i-p}) \bmod(m), \quad (2)$$

where $a > b > ... > p > 0$.

Usually, the module of equations (1) and (2) are equal to the power of number 2 − m = 2^n. This greatly simplifies the hardware implementation of generators. With correct choice of coefficients *l,k*

I. The structure schema and the work principle of the new AFG

In the hardware implementation of algorithms in which the module is a prime number, the principles of constructing two-level frequency synthesizers with an arbitrary given step of changing the average value of the output frequency, which were proposed in [4], can be used. The structure schema of one of the possible variants of this AFG is presented in fig.1.

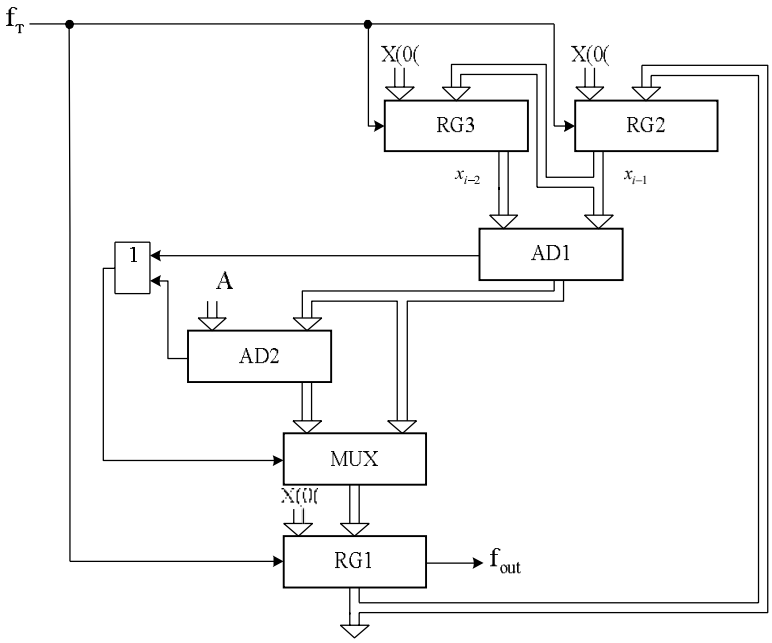

Fig. 1. Structure schema of AFG

It consists of: registers RG1 - RG3, adders AD1 - AD2, multiplexer MUX and logical element OR.

The generator functions in accordance with the equation:

$$x_i = (x_{i-2} + x_{i-1}) \bmod(m). \quad (3)$$

where m − prime number.

II. The structure schema and the work principle of the new AFG

In the hardware implementation of algorithms in which the module is a prime number, the principles of constructing two-level frequency synthesizers with an arbitrary given step of changing the average value of the output frequency, which were proposed in [4], can be used. The structure schema of one of the possible variants of this AFG is presented in fig.1.

The initial state of the generators is an array of initial values of the numbers x_i , $x_i - a$, $x_i - b$,..., $x_i - p$ corresponding to the initial registers settings in the hardware implementation of devices. This initial array (seed) is a cryptographic generator key. In most cases of using AFG and Modified Additive Fibonacci Generators (MAFG) [2, 3] there is a significant dependence of the statistical characteristics of the generated pseudorandom sequence from the initial settings, in particular, their dependence on the sequence repetition period [3]. This means the presence of so-called "weak keys", which could be relatively easily disclosed.

In this paper we present the results of research aimed at eliminating this deficiency of AFG. At the same time, the focus is on the hardware implementation of generators.

III. Researching the new AFG characteristics

In this paper we present the results of study of the dependencies of the pseudorandom sequence repetition periods from the initial generators' settings We also studied the dependencies of the statistical characteristics of the sequence using the NIST tests, which made it possible to formulate the possibility of using the developed devices as part of more advanced combined generators.

Fig. 2 shows the dependence of the repetition periods ofthe pseudorandom numbers sequence of investigated generators on the value of the key X(0).

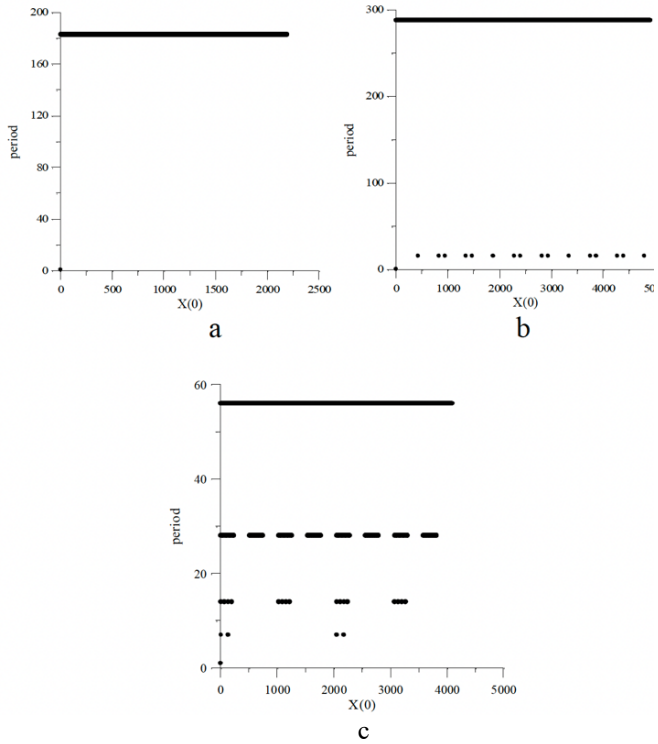

Fig. 2. Dependences of AFG repetition periodsfrom the key X(0)

Fig. 2 a, b represent the dependences for the new AFG (fig. 1), which works in accordance with equation (3): for m = 13 (fig. 2a) and for m = 17 (fig .2b). In fig. 2c, for comparison, the corresponding dependence for the classical AFG, which functions in accordance with equation (3) for m = 24 = 16 , is represented. In order to take all possible values, the initial number X(0) is determined by the formula:

$X(0) = x_{i-2}\,x_i(0)$, $x_{i-1}(0)$, $(0) + m \cdot x_{i-1}(0) + m \cdot x(0)$ (4)

where i x(0) , i-1 x (0) , i-2 x (0) − the initial values of the numbers in the registers RG1 - RG3 accordingly.

In this article, we present only some results of researching of different types AFG repetition periods.

During researching, a large number of AFG were analyzed at various values of the module *m* us to draw the following conclusions:

Tabl. 1 shows the values of the repetition periods of the new AFG output sequence (Fig. 1) for some values *m,* that are fixed on the whole set of possible values X(0).

TABLE 1

m	2	3	5	7	11	13	17	19
period	7	13	24 4	48 6	120 10	183	288 16	180 9
m	23	29	31	37	41	43	47	53
period	506 22	871	993	1368 36	1723	231 21	2257	1404
m	59	61	67	71	73	79	83	89
period	58	930	4488 66	5113	5403	3120	2296 82	3960 44
m	97	101	103	107	109	113	127	131
period	3116	100 50	3536	2862	1485	4256	16257	

Conclusion

New AFG (Fig. 1) constructed using prime numbers as modules of recurrent equations, at certain values of modules, provide the constancy of the repetition period of the output pseudorandom pulse sequence throughout the range of possible values of initial setups - keys (seed).

References

[1] Schneier B. Applied Cryptography. Protocols, algorithms, source code in C language. Moscow, Publishing House of the "Triumph", 2002, 797 p.

[2] 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. – 2014. – No 5. –Pp. 81-86.

[3] Harasymchuk O., Maksymovych V., Mandrona M., Kostiv Y. A study of the characteristics of the Fibonacci modified additive generator with a delay. Journal of Automation and Information Sciences. – 2016. – Vol.48, №11. – P. 76–82.

[4] Maksymovych VM, Stakhiv R.I. Analysis of the errors of the two-level frequency synthesizer. Bulletin of the Lviv Polytechnic National University - "Computer Engineering and Information Technologies", N496, 2003. - p. 17-22.