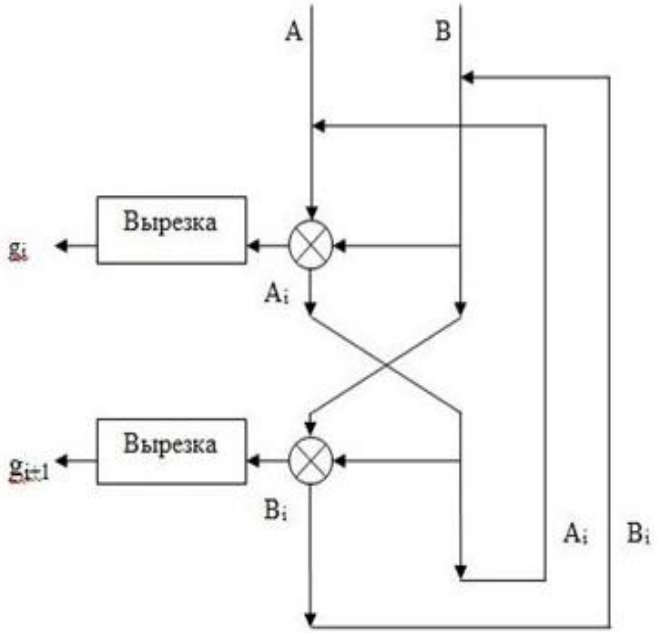
ИНСТИТУТ ИНФОРМАЦИОННЫХ И ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ КН МОН РК

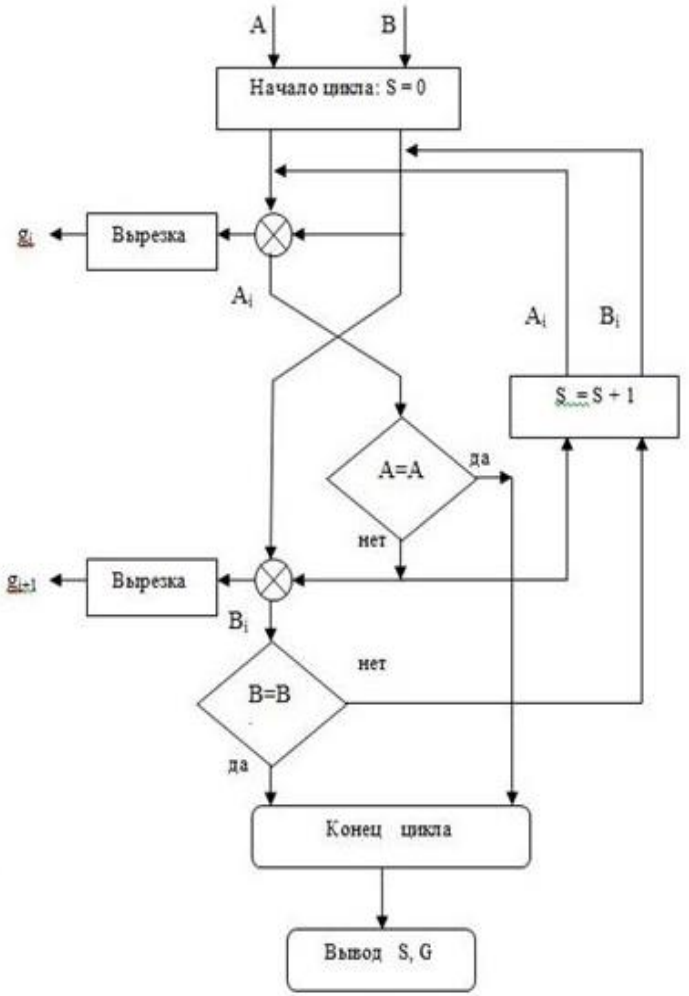
RESEARCH OF STATISTICAL PROPERTIES OF THE DEVELOPED PSEUDORANDOM SEQUENCE GENERATOR

K. Algazy, D. Dussenbayev

ALGORITHM FOR PSEUDORANDOM SEQUENCE GENERATING



a) PRS generation algorithm scheme



b) Generator scheme with periodicity check

PRINCIPLES OF CONSTRUCTION OF PRNG

Requirements for PRNG, oriented to use in information security systems :

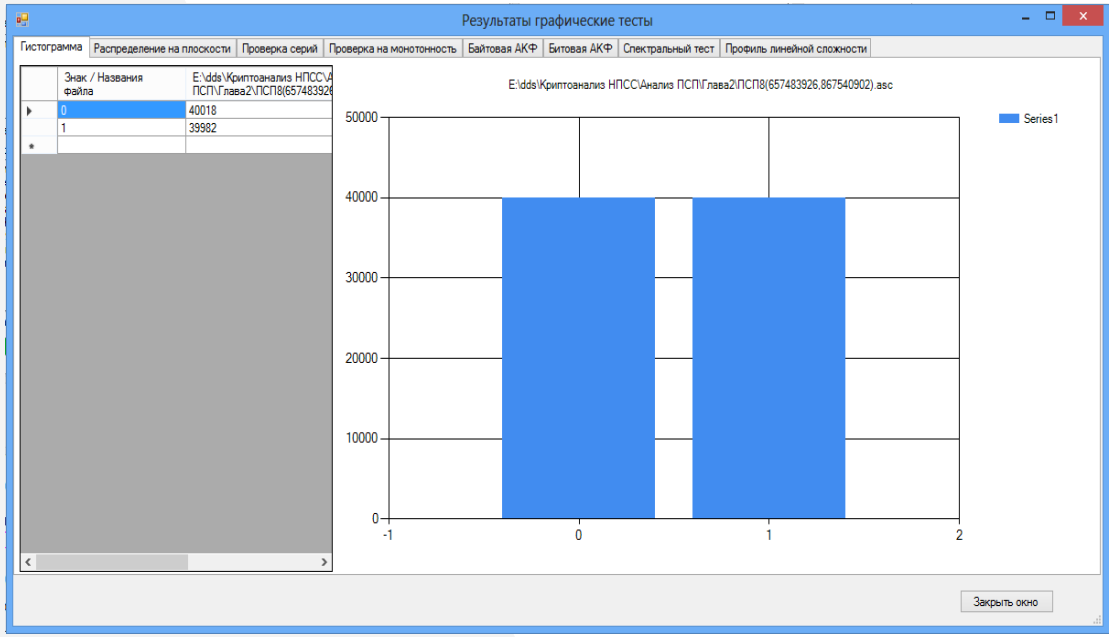
- Cryptographic strength;
- Good statistical properties;
- Large period of the formed sequence;
- Effective hardware and software implementation.

For the cryptographic PRNG, the following problems must be computationally unsolvable:

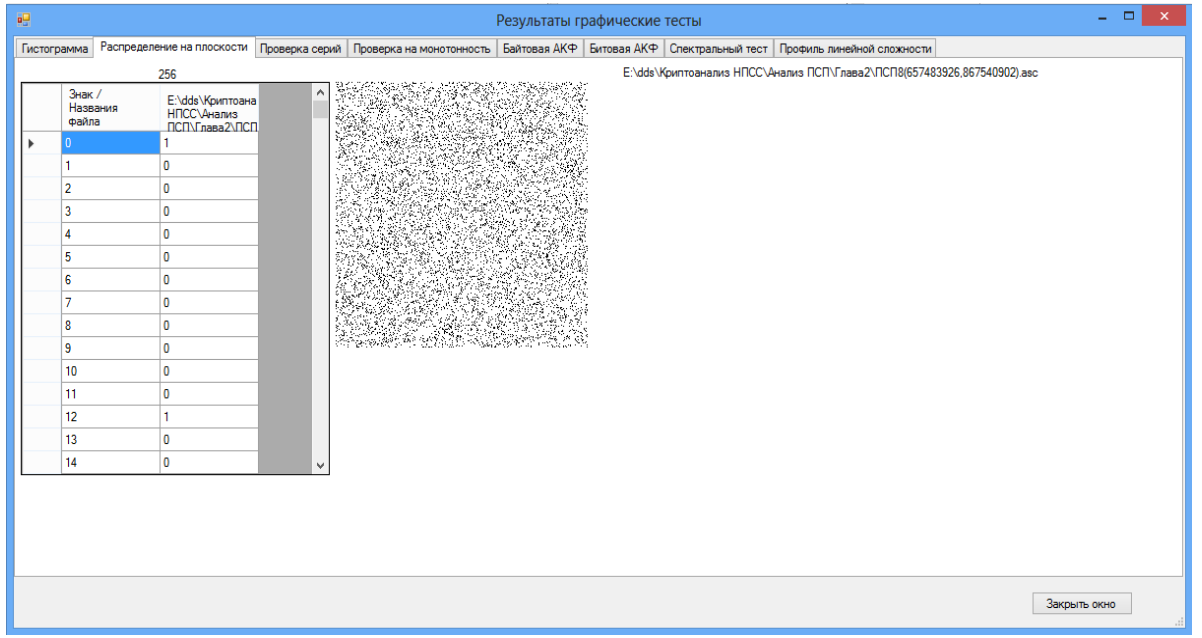
- the determination of (i-1)-th element of a sequence on the basis of a known fragment of finite length;
- the determination of (i+1)-th element of a sequence on the basis of a known fragment of finite length;
- determination of key information from a known fragment of a finite length.

TESTS RESULTS

«0» and «1» distribution



Distribution on a plane



TESTS RESULTS

№	Test	Chi-squared	Result
1	«0» and «1» distribution	0,0162	Test passed
2	Test of unconnected series	40,56	Test passed
3	Symbol check	222,4384	Test passed
4	Intervals check	3,2159	Test passed
5	Combinations check	1,5755	Test passed
6	Coupon collector’s test	11,1746	Test passed
7	Permutations test	130,6627	Test passed
8	Monotonicity test	19,0339	Test passed
9	Correlation test	No correlation	Test passed
10	Linear complexity test	29,015	Test passed

ASSESSMENT OF THE OFFSET OF “0” AND “1” OCCURRENCE PROBABILITY

Let’s consider the result of the multiplication operation and estimate the probability of occurrences of «0» and «1».

Let $A = a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0$, $B = b_m b_{m-1} b_{m-2} \dots b_2 b_1 b_0$ and their multiplication $C = c_{n+m-1} c_{n+m-2} \dots c_2 c_1 c_0$

Then

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 \qquad (1)$$

$$\dots\dots$$

$$c_{n+m-1} = a_n b_m$$

ASSESSMENT OF THE OFFSET OF “0” AND “1” OCCURRENCE PROBABILITY

Binary multiplication

	00	01	10	11
00	0000	0000	0000	0000
01	0000	0001	0010	0011
10	0000	0010	0100	0110
11	0000	0011	0110	1001

Probability of c_i become «1»:

$$P(c_0 = 1) = \frac{1}{4},\ P(c_1 = 1) = \frac{3}{8},\ P(c_2 = 1) = \frac{3}{16},\ P(c_3 = 1) = \frac{1}{16}$$

Rewrite the expression (1) as follows :

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 \oplus a_1 b_0$$

$c_2 = a_0 b_2 \oplus a_1 b_1 \oplus a_2 b_0 \oplus R_1$ *здесь* $R_1 = a_0 b_1 a_1 b_0$

. . . . . .

$c_{n+m-1} = a_n b_m \oplus R_{n+m-2}$

The probability of c_i become «1» in finite expressions:

$$P(c_0 = 1) = P(a_0 b_0 = 1) = P(a_0 = 1)P(b_0 = 1) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$$

$$P(c_1 = 1) = P(a_0 b_1 \oplus a_1 b_0 = 1) = P(a_0 b_1 = 0, a_1 b_0 = 1) + P(a_0 b_1 = 1, a_1 b_0 = 0) == \frac{3}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot$$

$$\frac{3}{4} = \frac{3}{8}$$

$$P(c_2 = 1) = P(a_1 b_1 \oplus a_0 b_0 a_1 b_1 = 1) = P(a_1 b_1 = 0, a_0 b_0 a_1 b_1 = 1) +$$

$$+P(a_1 b_1 = 1, a_0 b_0 a_1 b_1 = 0) = P(a_1 b_1 = 0) P_{a_1 b_1 = 0}(\, a_0 b_0 a_1 b_1 = 1) +$$

$$+ P(a_1 b_1 = 1) P_{a_1 b_1 = 1}(\, a_0 b_0 a_1 b_1 = 0) = 0 + \frac{1}{4} \cdot \frac{3}{4} = \frac{3}{16}$$

$$P(c_3 = 1) = P(a_0 b_0 a_1 b_1 = 1) = P(a_0 = 1)P(b_0 = 1)P(a_1 = 1)P(b_1 = 1) = \frac{1}{16}$$

General form of c_i : $c_i = \oplus \sum_{k+l=i} a_k b_l$

If $P(a_i = 0) = P(a_i = 1) = P(b_i = 0) = P(b_i = 1) = \frac{1}{2}$

then $P(a_k b_l = 0) = \frac{3}{4}$ и $P(a_k b_l = 1) = \frac{1}{4}, 1 \le k \le n, 1 \le l \le m.$

First, consider the case when there is no a carry digit transfer. We can use the following formula:

$$P\left(\oplus \sum_{k,l} a_k b_l = 0\right) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

or

$$P\left(\oplus \sum_{k,l} a_k b_l = 0\right) = \sum_{k=0}^{[\frac{n}{2}]} C_n^{2k} p^{2k} q^{n-2k}$$

The offset of the probability from 0,5 for the interval obtained with the generation algorithm is 0,0001 – 0,0002

0 :- 0,75
1 :- 0,375
2 :- 0,5625
3 :- 0,46875
4 :- 0,515625
5 :- 0,4921875
6 :- 0,50390625
7 :- 0,498046875
8 :- 0,5009765625
9 :- 0,49951171875
10 :- 0,500244140625
11 :- 0,4998779296875
12 :- 0,50006103515625
13 :- 0,499969482421875
14 :- 0,500015258789063
15 :- 0,499992370605469
16 :- 0,500015258789063
17 :- 0,499969482421875
18 :- 0,50006103515625
19 :- 0,4998779296875
20 :- 0,500244140625
21 :- 0,49951171875
22 :- 0,5009765625
23 :- 0,498046875
24 :- 0,50390625
25 :- 0,4921875
26 :- 0,515625
27 :- 0,46875
28 :- 0,5625
29 :- 0,375
30 :- 0,75

Now, consider the case where there is a carry digit transfer.

Then, $c_i = \oplus \sum_{k+l=i} a_k b_l \oplus R_{i-1}$, where R_{i-1} is a value from the lower digits. The regularity of its transfer is as follows:

$$P(R_{i-1} = 1) = C_{i-1}^{2} \left(\frac{1}{4}\right)^{2} \left(\frac{3}{4}\right)^{i-3} + C_{i-1}^{3} \left(\frac{1}{4}\right)^{3} \left(\frac{3}{4}\right)^{i-4} + \cdots +$$

$$C_{i-t}^{2t} \left(\frac{1}{4}\right)^{2t} \left(\frac{3}{4}\right)^{i-3t} + C_{i-t}^{2t+1} \left(\frac{1}{4}\right)^{2t+1} \left(\frac{3}{4}\right)^{i-3t-1}$$

0 :- 0,25
1 :- 0,375
2 :- 0,5546875
3 :- 0,478515625
4 :- 0,507568359375
5 :- 0,497698783874512
6 :- 0,500541388988495
7 :- 0,499943965813145
8 :- 0,499967868275249
9 :- 0,500025807115716
10 :- 0,499989382267968
11 :- 0,500002292975503
12 :- 0,500000558034211
13 :- 0,499999017675514
14 :- 0,500000715106658
15 :- 0,499999591625646
16 :- 0,500000209075493
17 :- 0,499999588443418
18 :- 0,500000553402205
19 :- 0,499999204665269
20 :- 0,500001327650118
21 :- 0,499998081047055
22 :- 0,500001185053007
23 :- 0,500005354598003
24 :- 0,49997269635432
25 :- 0,500072756039334
26 :- 0,499901445600516
27 :- 0,49981475594015
28 :- 0,5019093335733366
29 :- 0,49143905376191
30 :- 0,529313072562218
31 :- 0,41473388671875
32 :- 0,28125
33 :- 0

THANK YOU!

Institute of Information and Computational Technologies
Committee of Science
Ministry of Education and Science of Kazakhstan

iict.kz

e-mail:

dimash_dds@mail.ru, kunbolat@mail.ru