**DOI 10.12851/EESJ201508C05ART08**

***Gregoriy V. Kosovan***,
*ScD student;*

***Ruslan L. Politanskij***,
*ScD,*
*Yuriy Fedkovych*
*Chernivtsi National University;*

***Nazar G. Hladun***,
*co-founder;*
*LLC UKRINGROUP*

# Research of Binary Sequences Statistical Properties Generated on Chaotic Mappings

***Key words:*** *chaotic, binary, mapping*

***Annotation:*** *Cryptographic techniques provide protection and sustainable development of new algorithms for encrypting information based on theory of deterministic chaos. In this work displayed the results of researches which based on statistical properties of sequences generated on one-dimensional logistics, square and cubic maps.*

**Introduction**

In terms of applications in cryptography chaotic generators investigated the sensitivity to initial conditions and parameters. The main complication using random generators in cryptography is continuity and infinity space values while the classic technique of encryption operates discrete, limited space.

In this work displayed the results of researches which based on statistical properties of sequences generated on one-dimensional logistics, square and cubic maps. Pseudorandom sequence formed by the two steps. The first step is that random value generated from the sequence which compared with the value of the threshold decision. If it is greater than the threshold decision then it get logical "1", and if less - logical "0". The essence of the second step is a binary representation of member value generated sequence.

For research were used three-dimensional variables generated by maps (logistics, square and cubic) from randomly selected iterations (1). The equations of generators are shown in Table 1. Calculation in research used precision 15 decimal places.

Table 1

| Generator Type | Logistic | Square | Cubic |
|---|---|---|---|
| Equation of | $x_{n+1} = rx_n\left(1-x_n\right)$ | $x_{n+1} = 1-\mu x_n^2$ | $x_{n+1} = a-bx_n+x_n^3$ |

| generator | | | |
|---|---|---|---|
| Variables | $x_n$ - dynamical variable<br>$r$ - control parameter | $x_n$ - dynamical variable<br>$\mu$ - control parameter | $x_n$ - dynamical variable<br>$a$ , $b$ - control parameters |
| Conditions | Interval for $r$<br>$(3,65;4]$ | Interval for $\mu$<br>$(1,4;2]$ | Interval for $a$ - $[-0,6;0,6]$<br>Interval for $b$ - $[1,7;2,5]$ |

The algorithm of calculations contain three steps:

1. Entering of initial conditions and control parameters for one-dimensional maps.
2. Choosing of three changing maps ( research of periodicity ).
3. Setting accuracy calculations starting from the second decimal place before the 15th conducted repeated solutions of one-dimensional maps to regain the selected variable.

Repetition period is a number of iterations in which there was a re-generation of value. In Table 2 is presented the research of recurrence period of cube map.
All three dynamic systems implemented in the software environment Free Pascal, which allowed investigating the frequency of one-dimensional maps for different values of the initial conditions and different setting their accuracy.

Table 2

| Number of decimal places | $n_{25}$ = -0,649438673022647 | $n_{30}$ = -0,364884673132821 | $n_{100}$ = 1,19553863655266 |
|---|---|---|---|
| | Repetition period (interations) | Repetition period (interations) | Repetition period (interations) |
| 2 | 37 | 50 | 239 |
| 8 | 9440839 | 26631503 | 14945672 |
| 9 | 59393866 | 26631503 | 61218434 |
| 10 | >100000000 | >100000000 | >100000000 |

Obtained results suggest that the period of re-generating increasing faster for sequences generated by square and cubic mapping (in meaning if the accuracy of the calculation increase).

**Practical part (research)**

Each sequence has length of 16000000 bit. The calculation accuracy is 10 decimal places. The value of initial conditions and parameters for maps equations are shown in Table 3.

Table 3

| | First step of research | | | Second step of research | | |
|---|---|---|---|---|---|---|
| Type of map | logistic | square | cubic | logistic | square | cubic |

| | | | | | | |
|---|---|---|---|---|---|---|
| Initial condition | $x_0 = 0,1$ | $x_0 = 0,1236$ | $x_0 = 0,1347$ | $x_0 = 0,1364$ | $x_0 = 0,1$ | $x_0 = 0,05$ |
| Control parameters | $r = 3,95$ | $\mu = 2$ | $a = 0,2491$<br>$b = 2,61222$ | $r = 3,64933$ | $\mu = 1,9$ | $a = 0,3$<br>$b = 2,5$ |
| Threshold level | 0,5 | 0 | 0,6 | | | |

The length of cycles generated by different sequences of pseudorandom gene- rators are shown in Table 4.The results of the testing by ENT program are shown in Table 5 (2).

Table 4

| | First step of research | | | Second step of research | | |
|---|---|---|---|---|---|---|
| Type of map | logistic | square | cubic | logistic | square | cubic |
| Length of cycle | 22 | 106 | 110 | 18 | 23 | 21 |

Table 5

| | First step of research | | | Second step of research | | |
|---|---|---|---|---|---|---|
| Type of map | logistic | square | cubic | logistic | square | cubic |
| Ratio "1" and "0" | 0.499999<br>0.500001 | 0.497526<br>0.502474 | 0.684543<br>0.315457 | 0.502487<br>0.497513 | 0.505123<br>0.497877 | 0.504897<br>0.495103 |
| Entropy | 0.896038 | 0.896390 | 0.899372 | 0.895684 | 0.896364 | 0.896733 |
| The value of chi-square distribution | 203200000.02 | 2032050120.31 | 2310988670.47 | 2032050676.54 | 203203797.48 | 2032196419.02 |
| Arithmetic mean | 0.3125 | 0.3128 | 0.3356 | 0.3122 | 0.3128 | 0.3131 |
| Monte Carlo test | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 | 4.0 |
| Correlation coefficient | 0.000222 | 0.003723 | 0.055589 | -0.005999 | -0.005670 | -0.006911 |

To conduct statistical studies of each generators set was used statistical tests NIST STS 1,6 (3). Test results of test for first step are shown in Table 6 and for the second step are shown in Table 7.

From these results it can be concluded that the best statistical properties were produced by the first research step.

Table 6

| Type of test | Logistic map | Square map | Cubic map |
|---|---|---|---|
| Frequency test | 0.834308 | 0.152377 | 0 |
| Frequency test (blocks) | 0.772760 | 0.203934 | 0 |
| Batches test | 0.911413 | 0.221797 | 0 |
| Longest batches test | 0.437274 | 0.439162 | 0 |
| Rank of binary matrices | 0.041438 | 0.350485 | 0.438553 |
| DFT test | 0.037157 | 0 | 0.769024 |
| Template test | 0.350485 | 0.262978 | 0.222431 |
| Template 2 test | 0.744943 | 0.168790 | 0 |
| UMM test | 0.291003 | 0.201678 | 0.026545 |
| Lempel-Ziva test | 0.605408 | 1.000000 | 1.0 |
| Linear complexity | 0.378138 | 0.264458 | 0.500934 |
| Batches 2 test | 0.723129 | 0 | 0 |
| Entropy approximation | 0.378138 | 0 | 0 |
| TCS | 0.162606 | 0.158989 | 0 |
| RGT | 0.122325 | 0 | 0 |
| RGT 2 | 0.350485 | 0 | 0 |

Table 7

| Type of test | Logistic map | Square map | Cubic map |
|---|---|---|---|
| Frequency test | 0.069897 | 0.534375 | 0.069897 |
| Frequency test (blocks) | 0.198289 | 0.748869 | 0.198289 |
| Batches test | 0.118470 | 0.165623 | 0.118470 |
| Longest batches test | 0.396914 | 0.128379 | 0.396914 |
| Rank of binary | 0.232760 | 0.048716 | 0.232760 |

| | | | |
|---|---|---|---|
| matrices | | | |
| DFT test | 0.756476 | 0.860955 | 0.756476 |
| Template test | 0.407091 | 0.051391 | 0.407091 |
| Template 2 test | 0.577052 | 0.085369 | 0.577052 |
| UMM test | 0.162606 | 0.013808 | 0.162606 |
| Lempel-Ziva test | 1.0 | 1.0 | 1.0 |
| Linear complexity | 0.242986 | 0.222869 | 0.242986 |
| Batches 2 test | 0.432842 | 0.029796 | 0.432842 |
| Entropy approximation | 0.031534 | 0.044492 | 0.031534 |
| TCS | 0.029186 | 0.143561 | 0.029186 |
| RGT | 0.732713 | 0.534146 | 0.732713 |
| RGT 2 | 0.627783 | 0.122325 | 0.406181 |

**Conclusion**

1. Sequences generated by cubic map for the first step does not satisfy the conditions and as a result they satisfy the requirements of a small number of tests. This indicates the low efficiency of the first step using cubic map.
2. The results of statistical tests indicate pseudorandom type of sequence (pseudo sequence should have a small cycle length).
3. Pseudorandom sequence generated by the second step satisfies the requirements of security. It allows using these generators in secure communication systems.

**References:**


1. *Dmitriev AS, Panas AI. Dynamic chaos: novel type of information carrier for communication systems. Moscow, 2002; 252.*
2. *Ghandehari LS, Czerwonka J, Lei Y, Shafiee S, Kacker R. and Kuhn R. An Empirical Comparison of Combinatorial and Random Testing: 3rd Intl Workshop on Combinatorial Testing, Cleveland, OH, Mar. 2014.*
3. *Kuhn R, Kacker R, Lei Y. and Hunter J, Combinatorial Software Testing, IEEE Computer, vol. 42, no. 8, August 2009; 94-96.*