

# Encryption algorithm designing based on the dynamic chaos methods with discrete maps

Sidorenko A. V. and Mulayrchik K. S.

*Radiophysics Department, Belarusian State University, Minsk, Belarus*

In modern information systems the dynamic chaos methods are extensively spreading to become most promising research directions of an interdisciplinary nature, combining the elements from different theories such as information theory, dynamic systems theory, etc [1,2]. The studies of the use of dynamic chaos in cryptography have contributed to the emergence of new cryptographic primitives which are based on the elements of chaotic dynamics, in particular, on the discrete chaotic map [3]. Because of this, building of encryption systems with the use of such maps is a challenging task.

The main goal of this research is to develop the design principles for the encryption algorithms based on discrete chaotic maps and also the analytical methods for their cryptographic strength.

To meet this goal, the following tasks have been accomplished:

- Building of the data encryption scheme using a discrete chaotic map;
- Development of the software to implement the encryption scheme;
- Analysis of the algorithm stability to statistical attacks and a brute force attack

Let's proceed to the design of an encryption system (Fig. 1).

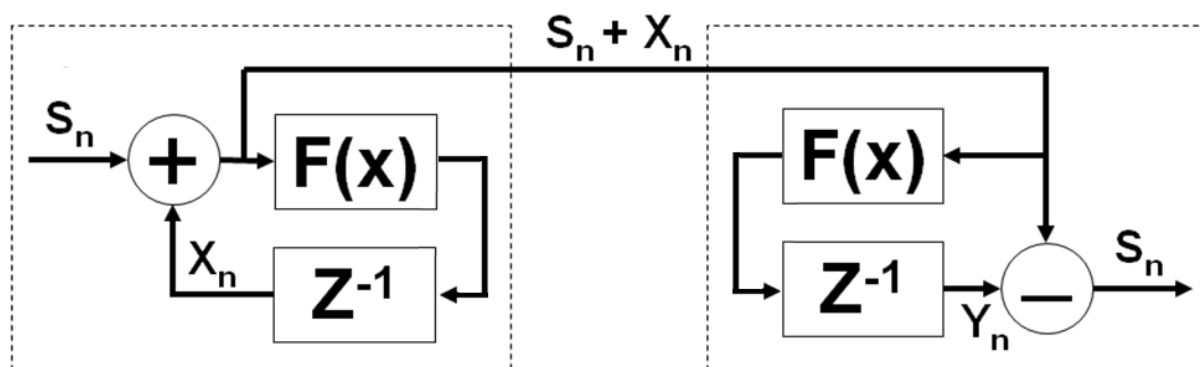


FIG. 1.

The encryption system shown in Fig. 1 is based on the phenomenon of self-synchronization of two chaotic systems and appears to be a scheme with a nonlinear mixing of the information

and chaotic signals [1]. Here  $F(X)$  is a non-linear transformation (a discrete chaotic map), and  $Z^{-1}$  – feedback filter, with a unit delay. The signal coming to the input of the transmitter passes through a nonlinear inverter and a feedback loop to be mixed with the signal arriving at the input of the transmitter and fed to the output. The scheme of the receiver is symmetric with respect to the transmitter operation.

A discrete tent-map was involved as a discrete chaotic map. This mapping may be described as follows:

$$F(X) = \begin{cases} \lceil \frac{A}{M}X \rceil, & 1 \leq X < M; \\ \lfloor \frac{A}{A-M}(A - X) + 1 \rfloor, & M \leq X \leq A \end{cases}$$

Also, the software that implements the described encryption scheme has been developed.

Now let's consider the problem of the encryption algorithm cryptographic security. In theory, there are several fields of cryptographic research: theoretical, practical, mimic resistance. The research of practical reliability is carried out by the stability of the technical and analytical cryptographic attacks [4].

The cryptographic strength of the developed encryption algorithm we have studied from the viewpoint of the

- frequency cryptanalysis
- resistance to brute force attacks/

Now consider the frequency cryptanalysis of the algorithm. The following Figure shows a comparison of spectra for a plaintext and ciphertext resultant from encryption of the plaintext. (Fig. 2) [5]. Here, the X-axis displays a symbol code, the Y axis - frequency at which this symbol occurs in the text.

As seen, a spectrum of the plain text (shown in blue) has the structure typical for this language. In turn, a spectrum of the ciphertext is a uniform noise.

To allow for comparative analysis of different variants of the scheme, the reliability of information hiding is estimated quantitatively. To this end, we introduce the correlation coefficient for spectra of the cipher text and plaintext. Empirically, a threshold for this coefficient is equal to 0.003 and, when the coefficient is less than 0.003, the cipher text spectrum does not exhibit any spectral structure of the plaintext.

The calculation results for the correlation coefficient of this scheme and for different encryption keys are as follows:

It is seen from this table that for the whole range of possible keys this coefficient is never exceeding a certain threshold and hence the scheme is resistant to the frequency cryptanalysis.

Then we proceed to analysis of the scheme stability to a brute force attack. For this purpose, we define an area in the formed key (region R), where errors are possible. The result of decryption

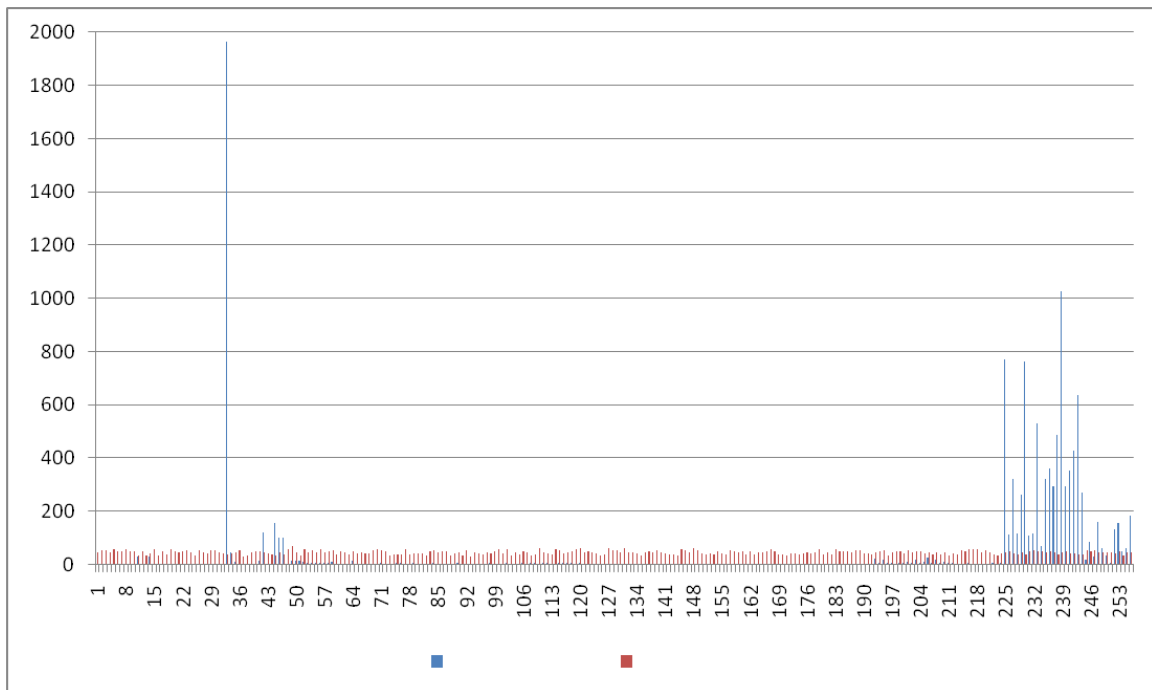


FIG. 2.

Key, M	Correlation coefficient, k
0x0000000000000001	0,002949
0x1111111111111111	0,001559
0x2222222222222221	0,001505
0x3333333333333331	0,001682
0x4444444444444441	0,001622
0x5555555555555551	0,001573
0x6666666666666661	0,001204
0x7777777777777771	0,00142
0x8888888888888881	0,00136
0x9999999999999991	0,001561
0xAAAAAAAAAAAAAAAAA1	0,001239
0xBBBBBBBBBBBBBBBBB1	0,001507
0xCCCCCCCCCCCCCCC1	0,001427
0xDDDDDDDDDDDDDDD1	0,001811
0xEEEEEEEEEEEEEEEEE1	0,001717
0xFFFFFFFFFFFFFFFFF	0,001946

when using this key with wrong bits is close to the source. A size of this area is defined in bits and is a quantitative characteristic of the encryption system resistance to a brute force attack.

Let us estimate a size of the region R for the designed encryption scheme:

Key, M	R region size, bit
0x0000000000000000	62
0x1111111111111111	62
0x2222222222222222	62
0x3333333333333331	62
0x4444444444444441	61
0x5555555555555551	61
0x6666666666666661	61
0x7777777777777771	61
0x8888888888888881	61
0x9999999999999991	61
0xAAAAAAAAAAAAAAAAA1	61
0xBBBBBBBBBBBBBBBB1	61
0xCCCCCCCCCCCCCCC1	61
0xDDDDDDDDDDDDDDDD1	62
0xEEEEEEEEEEEEEEEE1	62
0xFFFFFFFFFFFFFFFFF	62

It is seen that a size of the region R for the whole range of possible encryption keys is close to the key length (64 bit), indicating that the scheme is not resistant to brute force attacks.

To eliminate this deficiency and ensure the stability of this scheme to an attack by brute force, we propose a modification of the encryption scheme, replacing a single application of the chaotic map with a sequence of n applications. The resultant scheme is shown in Fig. 3.

Let's assess the stability of the modified scheme to the frequency cryptanalysis as well as to brute force attacks. The Table below lists the correlation coefficients for different values of the encryption key and various applications of the chaotic map.

In the Table below a size of the region R is given for different values of the encryption key and various applications of the chaotic map.

As seen from this table, at certain combinations of the encryption key and for some applications of the chaotic map a size of the region R is equal to zero. This, in turn, suggests that the scheme is resistant to brute force attack. Also, the experiment performed suggests that for each key size there are some applications of the chaotic map, for which the scheme is resistant to brute force attacks.

To summarize it all:

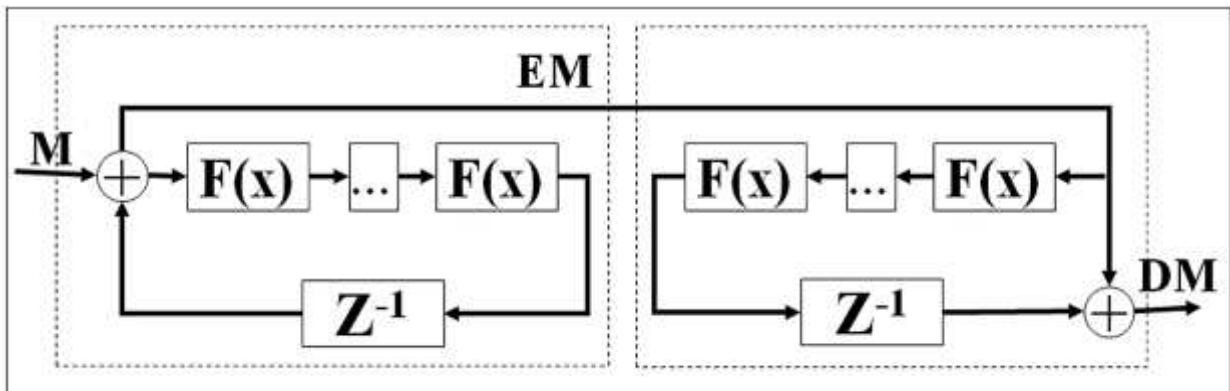


FIG. 3.

Key, M	Applications of the chaotic map, n								
	1	10	20	30	40	50	60	70	80
0x0000000000000001	0,0029	0,0472	0,0648	0,0494	0,0020	0,0065	0,0516	0,0305	0,0017
0x1111111111111111	0,0015	0,0015	0,0013	0,0014	0,0015	0,0017	0,0016	0,0013	0,0014
0x2222222222222221	0,0015	0,0015	0,0016	0,0015	0,0015	0,0014	0,0016	0,0016	0,0014
0x3333333333333331	0,0016	0,0016	0,0016	0,0017	0,0014	0,0013	0,0013	0,0016	0,0014
0x4444444444444441	0,0016	0,0016	0,0015	0,0015	0,0013	0,0014	0,0015	0,0015	0,0014
0x5555555555555551	0,0015	0,0013	0,0015	0,0015	0,0016	0,0014	0,0013	0,0014	0,0015
0x6666666666666661	0,0012	0,0014	0,0016	0,0014	0,0016	0,0014	0,0014	0,0015	0,0014
0x7777777777777771	0,0014	0,0013	0,0015	0,0015	0,0014	0,0014	0,0016	0,0016	0,0012
0x8888888888888881	0,0013	0,0016	0,0012	0,0015	0,0015	0,0016	0,0015	0,0012	0,0014
0x9999999999999991	0,0015	0,0015	0,0016	0,0013	0,0015	0,0016	0,0015	0,0015	0,0012
0xAAAAAAAAAAAAAAAAA1	0,0012	0,0015	0,0013	0,0014	0,0012	0,0016	0,0018	0,0014	0,0014
0xBBBBBBBBBBBBBBBBB1	0,0015	0,0015	0,0014	0,0013	0,0015	0,0016	0,0015	0,0012	0,0014
0xCCCCCCCCCCCCCCC1	0,0014	0,0016	0,0014	0,0011	0,0016	0,0013	0,0016	0,0013	0,0015
0xDDDDDDDDDDDDDDD1	0,0018	0,0014	0,0018	0,0013	0,0014	0,0011	0,0016	0,0016	0,0014
0xEEEEEEEEEEEEEEEEE1	0,0017	0,0015	0,0014	0,0014	0,0013	0,0016	0,0013	0,0016	0,0014
0xFFFFFFFFFFFFFFFFF	0,0019	0,0017	0,0102	0,0043	0,0016	0,0103	0,0101	0,0029	0,0023

1. An encryption system using the methods of dynamic chaos has been designed.
2. The features of discrete chaotic maps used in the encoding scheme have been investigated.
3. The software for operation of the proposed system has been developed.
4. A reliability analysis has been conducted, and the criteria have been stated for the encryption scheme to be resistant to some types of cryptographic attacks.

Key, M	Applications of the chaotic map, n								
	1	10	20	30	40	50	60	70	80
0x00000000000000001	62	59	58	57	57	56	56	56	56
0x11111111111111111	62	57	53	50	47	44	40	38	35
0x22222222222222221	62	55	50	45	39	34	29	23	18
0x33333333333333331	62	54	47	40	33	26	19	12	6
0x44444444444444441	61	53	45	36	28	21	12	4	0
0x55555555555555551	61	53	44	34	25	16	7	0	0
0x66666666666666661	61	52	42	33	23	13	4	0	0
0x77777777777777771	61	52	42	32	22	12	3	0	0
0x88888888888888881	61	52	42	32	22	12	3	0	0
0x99999999999999991	61	52	42	33	22	13	4	0	0
0xAAAAAAAAAAAAAAAAA1	61	52	43	34	25	15	7	0	0
0xBBBBBBBBBBBBBBBBB1	61	53	45	36	28	20	11	4	0
0xCCCCCCCCCCCCCCC1	61	54	46	40	33	25	19	12	5
0xDDDDDDDDDDDDDDDD1	62	54	49	44	39	34	28	23	18
0xEEEEEEEEEEEEEEEEE1	62	56	53	49	46	43	39	37	34
0xFFFFFFFFFFFFFFFFF1	62	59	58	57	57	57	56	56	56

## References

- [1] [1] A. S. Dmitriev, A. I. Panas Dynamic chaos. New carriers of information for communication systems. M.: Fizmatlit, 2002. – 205 p.
- [2] A. V. Sidorenko Information aspects of nonlinear dynamics. Minsk: BGU, 2008. – 125 p.
- [3] J. M. Amigo, L. Kosarev, J. Szczepanski. Theory and practice of chaotic cryptography. – Phys. Lett. A , - 2007. V.366. - P.211-216.
- [4] A. P. Alferov. Basics of cryptography. / A.P. Alferov, A.Yu..Zoubov, A.S. Kuz'min, A.V. Chermushkin. Moscow: Helios ARV, 2005 – 480p.
- [5] A. V. Sidorenko, K. S, Mulayrchik K. S. Analysis of the cryptographic strength of algorithm based on dynamic chaos // Information systems and technologies / Proc. of the International conference-forum IST' 2009. Nov. 16-17, 2009 Minsk: BGU. Part.II. – P.75-76.