THE ANALYSIS OF THE AVALANCHE EFFECT IN DISCRETE CHAOTIC MAPS FOR BLOCK CIPHERS

A.V. Sidorenko, K.S. Mulyarchik
Belarusian State University
Minsk, Republic of Belarus
e-mail: sidorenkoa@yandex.ru

Intensive development of information technologies and their penetration to all spheres of human life raises the concerns of information security to a new level. There is a strong need in encryption algorithms compatible with new technologies, such as, clound-computing. In this regard, the development of encryption algorithms based on a dynamic chaos is of particular interest [1,4].

Cryptographic security of the encryption algorithms based on a dynamic chaos is analyzed with the use of both standard and specialized approaches [1,2], differential cryptanalysis being one of the most extensively employed [3]. Thus, one of the key requirements for the encryption algorithm to be resistable to differential cryptanalysis is the occurrence of the avalanche effect in the base transformation. This effect is exhibited as a significant ("avalanche") change of output bits for a minor change (perturbation) of the input bits involved in the transformation as compared to the initial (unperturbed) values. The avalanche effect occurring in the base transformation makes it problematic to apply differential cryptanalysis technique. Good diffusion properties of an encryption algorithm are largely determined by the avalanche effect. The following criteria of cryptographic security are based on the avalanche effect [5]:

1. avalanche criterion (AVAL) requires a change, *on the average, of a half of the bits* in the output (ciphered) value for changing of every single bit in the input (initial) value

2. strict avalanche criterion (SAC) requires a change, *with the probability 0.5, of every single bit* in the output value for changing of every single bit in the input value

During the analysis of an encryption algorithm the above criteria may be applied both to the substitution node (S-block, map) and base transformation.

Changing of the output bits with the probability 0.5 is hardly possible in practice even in the case of the most cryptoresistable transformations. Because of this, a degree of the avalanche effect is characterized by the avalanche parameters representing numerical values of deviation of the output-bit change probability from the 0.5 [5]:

1. for avalanche criterion – $\varepsilon_{A_i} = |2k_{AVAL}(i) - 1|$,

2. for strict avalanche criterion – $\varepsilon_{S_{i,j}} = |2k_{SAC}(i,j) - 1|$.

In these expressions by i we denote the input bit number, by j – output bit number. The variability range of the parameters is 0..1. Values of the avalanche parameters which are closer to the lower limit of this range are associated with a stronger avalanche effect.

This work presents an analysis of the avalanche effect observed in a discrete tent map and in the base transformation based on the Feistel network with the use of the indicated map as a nonlinear function.

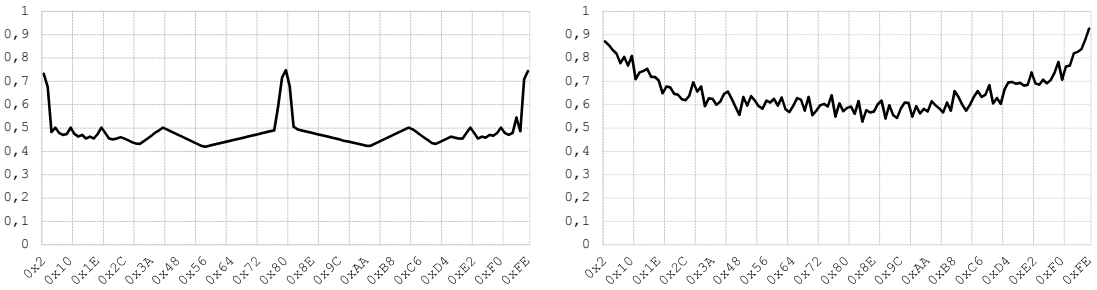
A discrete tent map onto the integer set $S = \{0, 1, ..., M-1\}$ of the power $M = 2^n$ (n – number of bits) is given by the following expression:

$$F(X) = \begin{cases} \left\lceil \frac{M}{A} X \right\rceil, 0 \le X \le A, \\ \left\lfloor \frac{M}{M-A}(M-X) \right\rfloor + 1, A < X \le M-1 \end{cases},$$

where X – input value, A – control parameter.

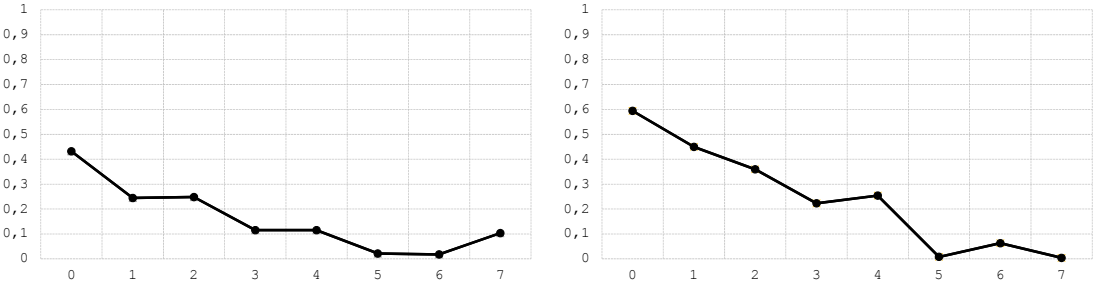
The avalanche effect for the mapping and the base transformation has been analyzed in the following cases:

1. perturbing input value X of the map at a fixed value of the control parameter A,
2. perturbing control parameter A at the fixed X.



(a) (b)

Fig. 1. Maximal value of the avalanche parameter ε_A (Y-axis) over all the output bits as a function of the control parameter A (X-axis) () and of the input value X (X-axis) (b) of a tent map. Power of the set – 8 bits.



(a) (b)

Fig. 2. The avalanche parameter ε_A (Y-axis) as a function of the input bit number (-axis) for the control parameter $A = 0x52$ () and for the input value $X = 0x52$ (b) of a tent map. Power of the set – 8 bits.

As seen from the curves (Fig.2), a value of the avalanche parameter ε_A is decreased as the bit number increases. It should be noted that the avalanche effect of tent map is observed more with a change of the input bits 5-8 than with a change of the bits 1-4. This fact points to weak diffusion properties of a discrete tent map.

Proceeding from the aforesaid, we can justify:

1. the type of the basic transformation – by analyzing avalanche effect in the pair input value – output value of a tent map;

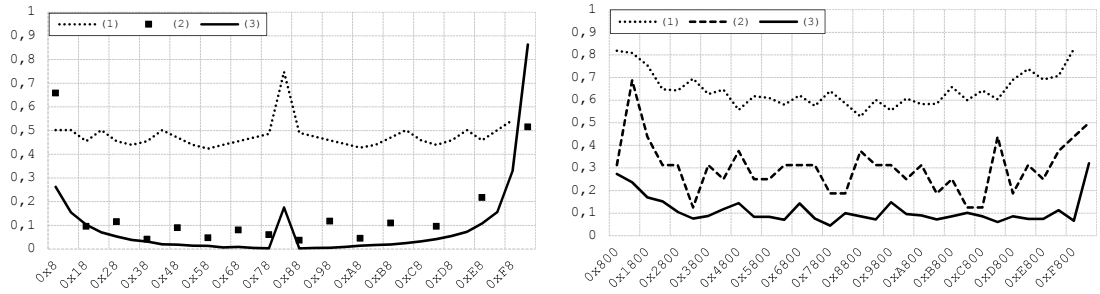
2. the round key generation schemes – by analyzing avalanche effect in the pair control parameter – output value of a tent map.

Based on the results of analysis, it has been demonstrated that the Feistel network is an appropriate form of the basic transformation.

Considering the structural features of the Feistel network, we can propose two variants to compare the avalanche effect in the initial discrete tent map and when it is used as a nonlinear function in the basic transformation. Thus, *map* onto a set with a power of *8 bits* may be compared to:

1. *the base transformation* of a set with a power of *8 bits*, where *the map itself* being defined onto a set of *4 bits*; in this case *a power of a set of the compared transformations is preserved*;

2. *the base transformation* of a set with a power of*16 bits*, the map itself being defined onto a set with a power of *8 bits*; in this case *a set is preserved that is used to define the initial map and used in the base transformation.*



(a) (b)

Fig. 3. Maximum value of the avalanche parameter ε_A (Y-axis) over all the output bits as a function of the control parameter A (-axis) () and of the input value X (-axis) (b) for the initial tent map onto a set with a power of 8 bits (curve 1), for the base transformation of a set with a power of 8 bits (curve 2), for the basic transformation of a set with a power of 16 bits (curve 3). The number of rounds for the base transformation is set to 10, the initial key is used in every round.

As seen from the curves (Fig.3), in the base transformation based on the Feistel network with a discrete tent mapping over particular ranges of control parameters and of input values one can observe a stronger avalanche than in the initial map. In this

way over the range of the control parameters 018 – 078 088 – $0xE8$ the corresponding values of the avalanche parameter ε_A for the basic transformation are within the interval 0-0.1, whereas for the initial map – within the interval 0.4-0.5. A lower value of the avalanche parameter suggests a stronger avalanche effect. Over the range of input values 02800 – $0F800$ the corresponding values of the avalanche parameter ε_A for the basic transformation are within the interval 0.05-0.15 and for the initial map – within the interval 0.5-0.75.

Thus, over the indicated ranges of the input values and of the control parameters one can state that the base transformation based on the Feistel network and the discrete tent map meet the requirements of the avalanche criterion providing resistability to differential cryptanalysis.

Conclusions:

1. The avalanche effect in a discrete tent map has been analyzed. It has been found that a tent map itself has a weak avalanche effect as the corresponding values of the avalanche parameter are greater than 0.4.

2. Considering that the avalanche parameter is irregularly dependent on the bit number in the input value, the Feistel network has been used as a type of the base transformation.

3. For the base transformation based on the Feistel network with a discrete tent map over the indicated ranges for the input values and for the control parameters, the requirements of the avalanche criterion are met providing resistability to differential cryptanalysis.

References

[1] Sidorenko A.V., Mulyarchik K.S. (2012). The control of chaotic regimes in encryption algorithm based on dynamic chaos. *Proc. of 16th International Conference-School Foundations. Advances in Nonlinear Science, Minsk, September 24-28, 2012, Belarusian State University*, p. 55.

[2] Sidorenko A.V., Mulyarchik K.S. (2012). Data encryption algorithm based on discrete chaotic systems and maps. *Technical means of information security: Proc. of Xth Belarusian-russian scientific conference, Minsk, May 29-30, 2012, Belarusian State University of Informatics and Radioelectronics*, pp. 50.

[3] Heys H.M. (2002). A tutorial on linear and differential cryptanalysis. *Cryptologia*. Vol. **26**, pp. 189-221.

[4] Kocarev L. (2001). Chaos-based cryptography: a brief overview. *Circuits and Systems Magazine, IEEE.*. Vol. **1**, pp. 6-21.

[5] Vergili I., Yücel M.D. (2001). Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen S-Boxes. *Turk J Elec Engin.*. Vol. **9**, pp. 137-145.