UDC 519.71

V.V. Kyrychenko, PhD, Ye.V. Lesina, PhD
(National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Ukraine)

Features of data protection algorithms based on dynamic systems

The computer algorithm realization of transformation information is based on chaotic dynamics and leads to necessity of discretization systems. The paper is dedicated to studying of specifics of inverse dynamic control systems as information transformers, in particular such their specifics like dynamic degradation. It involves the probable sudden decreasing of discrete state sets of complicated dynamic system, when the information statement is entered. This effect, for the most part, depend on the initial values of trajectory and system parameters.

Because of development satellite, mobile and computer communication systems, the significance of problem private data transfer is increasing and the wider problem of protecting information on the market of communication services also increases. At present the compulsive need in protecting commercial information in networking, supporting safe e-payment or IP telephony is formed. The typical request is the necessity wide appliance of encryption algorithms and their low prime cost per unit 'information' product. In the last time, with the appearance of paper [1], the possibilities of usage dynamic systems, which have chaotic behavior ([2, 3]), in telecommunication technologies are intensive studied.

The schemes of determined of unknown input by information about system output, which are true for continuous systems, can be used also for discrete system. The dynamics can be defined by the following equations:

$$\begin{aligned} x(k+1) &= f(x(k), u(k)), \\ y(k) &= h(x(k)). \end{aligned} \tag{1}$$

In the system (1) the output doesn't depend directly on input information sequence $u(k)$. Let's by analogy define the term of relative order input for continuous case. The function value $h\big(f(x,u)\big)$ may not depend on values u, so similarly

$$y(k+1) = h\big(f(x(k), u(k))\big)$$

may not contain $u(k)$. Defining what is the delay of steps between input and output system (1). This value points at relative sequence input in system (1).

Let's consider discrete realization of described dynamic system and set a problem to determine their characteristics as data-flow dynamic encryption of information sequence $\{u(k),\ k = 1,\ldots N\}$. The transition to the operations in integer field allows to remove a number of difficulties, which appeared when using discrete dynamic systems. The general problem is connected with fact that usage of multidimensional systems leads to superfluous calculations. When using machine arithmetic with floating point, the redundancy of computational operations over data array leads to: a) obvious growth of data process time; b) fast growth of computation error.

The computing device with fixed point provides much more speed of calculations without errors. Besides, such computing devices can be easily realized in the form of digital encryptor-decryptor, located in the places of input and output of flow data information system to general communication net.

Examine one-dimensional discrete system, the right sides of which don't depend on internal influence (the system modulation absence by information signal $u(k)$):

$$x(k+1) = F\big(x(k)\big)$$

Let the machine accuracy of computing device, that is used, is L bits. Then, any value A is represented in binary code, has the view A mod 2L. It means that values A are included in set {0,1,2,…,2L-1}. Following to that measure integer-valued points in space R^n is equal to zero, the dynamic system, is written in finite field with 2L elements, cannot valid describe dynamics of chaotic system, that caused it.

The next conclusion is the result of determinacy and the fact that state space x(k) is determined by 2L values {0,1,2,…,2L-1}:

Any system trajectory with initial condition x(0) in the field of integers in modulus 2L will be periodic with period TX(0), as a rule less than 2L. Therefore, one of the criterion of chaotic dynamic system - continuous spectrum of solutions – is not fulfilled. Integer-valued trajectory has discrete spectrum divisible by TX(0).

So, for the dynamic system in the field of integers in modulus 2L the chaotic masking method, where the signal, that is transferred, carries information in the form $y(k) = x(k) + u(k)$, doesn't change frequency properties of message $u(k)$.

References

1. Sobhy M. J. and Shehata A. Secure computer communication using chaotic algorithms // Int. J. of Bifurcation and Chaos. – vol. 10, no. 12, 2000. – P. 2831–2839.

2. Kirichenko V.V. *Information security of communication channel with UAV* // Electronics and control systems. – №3 (45), 2015. – P. 23-27

3. Kyrychenko V.V., Lesina Ye.V. *Application of dynamic systems for encoding data in telecommunication channels* // Electronics and control systems. – №3 (53), 2017. – P. 11-16