DIGITAL APPROXIMATIONS OF CHAOTIC SYSTEMS IN CRYPTOGRAPHY

L. Yu. Gerasimov

Information Systems Security Department, Samara State University, Acad. Pavlova 1, 443011, Samara, Russia,
gerasimovleo@gmail.com

Deterministic chaos systems possess two important properties. On the one hand they can demonstrate very complex noise-like behavior. On the other hand they are deterministic, thus their dynamics can be exactly reproduced, as long as exact parameters and initial conditions are known. These properties make deterministic chaos systems suitable to be used as basis for pseudo-random numbers generators in cryptography.

However, truly chaotic systems imply continuous phase space, while modern cryptography deals with digital systems that can provide only finite-state phase space. With such restrictions it is impossible to achieve infinite chaotic orbit. Sooner or later digital system will return in some of its previous state and the obit became a cycle. Moreover the nature of digital computing that includes rounding and truncating can make these cycles even shorter and totally unsuitable for cryptography practices.

The other task is conversion from chaotic dynamic system trajectory to random bits strings that are used in encryption algorithms. These strings should meet some strict requirements to guarantee information security. Sometime the easiest way to obtain random bits string from dynamic system trajectory results in strings with poor characteristics unsuitable for encryption. Thus more complex and sophisticated conversion algorithms required.

In the proposed research a program model of pseudo-random bits generator was designed and examined. As a basic deterministic chaos system the Van der Pol oscillator was used. It can be described by following differential equation:

$$\ddot{x} - \lambda(1 - x^2)\dot{x} + x = 0, \tag{1}$$

where $\lambda > 0$ is dimensionless control parameter.

For the sake of computer calculations a discrete time counterpart proposed in [1] was used. Each systems state obtained from previous two according equation:

$$y[n] = \alpha_1 y[n-1] + \alpha_2 y[n-2] + \gamma(1 - y^2[n-1])(y[n-1] - y[n-2]). \tag{2}$$

where n is discrete time, and α_1, α_2, and γ are control parameters. As well as for analogue prototype, for this discrete time system a chaotic mode exists. Control parameters range where system exhibits chaotic behavior was examined in [2].

Designed pseudo-random bits generator uses control parameters values as well initial conditions as a seed or a secret key. It computes chaotic orbit for a given iterations number and performs some post-processing transformations to obtain cryptographically secure bit strings. An example of chaotic trajectory without post-processing is given in Figure 1.

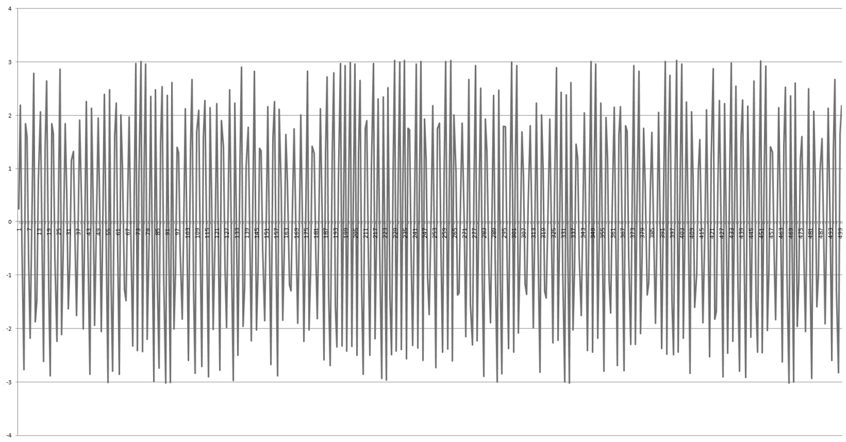

Figure 1: Chaotic orbit obtained with parameters: α_1 = 0.605, α_2 = -0.959, γ =0.195, $y[n\text{-}2]$=0, $y[n\text{-}1]$=0.5, N=500;

For post-processing algorithm design and result bit strings examination NIST statistical test suite [3] was used. According to tests passing results designed pseudo-random bits generator can produce cryptographically secure random bit strings.

REFERENCES

1. Zaitsev V.V., et al. The dynamics of the discrete auto-vibrations of the Van der Pol oscillator, Physics of wave processes and radio-technical systems, V. 3, №2, 2000. (In Russian).

2. Zaitsev V.V., et al. Statistical estimations of the stochastic oscillations characteristics of the discrete Van der Pol oscillator, Physics of wave processes and radio-technical systems, V. 4, №1, 2001. (In Russian).

3. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, NIST Special Publication 800–22, Revision 1a: April 2010, http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf