# Ph.D. Thesis Review

Name of student: Ing. Volodymyr Lynnyk
Title of the thesis: Chaos - based communication systems
Supervisor: Doc. RNDr. Sergej Čelikovský, CSc.
University: Czech Technical University in Prague
Faculty: Faculty of Electrical Engineering
Department: Department of Control Engineering

Contents:
The thesis presents a brief introduction to the theory of nonlinear dynamical systems with deterministic chaos, cryptography, chaos based communication and encryption, methods of analysis of the security of the chaotic encryption and possible methods of attack. The main contribution of the thesis is a new algorithm for secure communication, namely the anti-synchronization chaos shift keying (ACSK) scheme based on the generalized Lorenz system (GLS), including the security analysis. Also synchronization and communication in more complex networks is discussed.
This is a current topic with important possible application in secure communication. The chosen methods are appropriate and the results are of significant scientific value.
Own publications:
The list of references contains 9 publications of the author, one of them in Kybernetika (Impact factor 0.281 in 2008) and 8 contributions in proceedings of conferences in all five continents.
My analysis of the main result:
The main contribution of the thesis is the ACSK (anti-synchronization chaos shift keying) scheme using GLS (generalized Lorenz system) for secure communication. A sketch of a possible attack might look like this: A system of 3 ODE with 1 parameter is solved numerically with a fixed time step. This is equivalent to a discrete–time dynamical system

$$x^{new} = f(x^{old}, p).$$

A scalar function is used to generate the transmitted signal

$$y = g(x).$$

Thus the graph of $y$ as a function of $x$ is a 3–dim hyper-surface in a 4–dim space. This can be reconstructed from the scalar signal using the Takens delay theorem. The message in the form of a sequence of bits is used to switch between two values of the parameter $p$, say $p_1$ and $p_2$. As a result each of the four components of each point in the 4–dim space splits in two possible values, depending on the particular value of the parameter. This gives $2^4 = 16$ points. Thus instead of one 3–dim hyper-surface we have 16 hyper-surfaces. A possible intruder can detect these 16 hyper-surfaces if enough points are available. To be more precise to detect individual hyper-surfaces we need points to have close neighbors in the same hyper-surface. Denoting the difference of the two parameter values $\Delta p$ we can estimate the distance between the hyper-surfaces as

$$\epsilon = \sum_i \frac{\partial g}{\partial x_i} \frac{\partial f_i}{\partial p} \Delta p.$$

We need at least

$$N > (\frac{1}{\epsilon})^D$$

points, where $D$ is the capacity dimension of the attractor. If the intruder collects more than $N$ points he can identify the particular hyper-surface of each received point and from this information he can detect whether $p_1$ or $p_2$ was used. In this way he can decipher the message. To make the decipher process more difficult the sender can choose the parameter difference $\Delta p$ very small. Then the intruder needs a large number of points, possibly more than the length of the entire message. But then the signal becomes sensitive to noise, which becomes a problem even for the authorized receiver.

Formal level of the thesis:
The thesis contains interesting mathematical results with important possible application and analyzed with advanced theoretical methods. However, the formal level of the text is of lower quality. One more careful reading of the thesis would help. I have found 163 errors. To mention a few:

- In Fig. 2.1 the text in the Receiver box does not agree with (2.5).
- In (2.14) the second $s(t)$ should be $e(t)$.
- Page 48: "For all $\epsilon \geq 0$, assume $|\eta_1(t) - \eta_1^m(t)| \leq \epsilon$." means $\eta_1(t) = \eta_1^m(t)$. Rather "for a fixed $\epsilon \geq 0$" should be used.
- Page 49: $(n_1 \times 1)$ should be $(1 \times n_1)$ and $\varphi^1$ should be smooth for the last equation to be true.
- In (3.12) the last $+$ should be $-$.
- In (3.13) $x^2$ should be $y^2$.
- In (3.14) $\varphi^2$ should be $\varphi^1$.
- Page 53: it is not clear what $|s_{11}|e_1| + |s_{21}|e_2|$ means.
- Also, if $V$ is scalar it is not clear why $||\frac{dV}{dt}||$ is used. First I thought it should be $|\frac{dV}{dt}|$ but I do not understand why the formula in line 7 from the bottom implies $V(e)$ is strictly decreasing. Perhaps the $||.||$ should be omitted at all.
- In Fig 3.3 it is not clear what the two types of curves mean.
- Also the numbers along the horizontal axis are difficult to read.
- It is not clear why a network consisting of two nodes is called a complex network.
- In Theorem 3.6.2. it is not clear why the trajectory $\eta(t)$ is assumed to be uniformly bounded. In this case the term bounded is perfectly enough. The term uniformly is important in the case of infinitely many functions.
- (3.25)-(3.26) is not in the form of (3.23). If $c_{ij} = 0$ then (3.23) splits into $N$ isolated systems while (3.25)-(3.26) does not.
- In the proof of Theorem 3.6.2 the meaning of $\Theta$ is not clear.
- In the list of references some parts of the text are missing as in [4]: Conference on what? In [7] and [30] the type of publication and the publisher is missing. In [26] Solution should be Solitons. In [61] Rusian should be with double s.
- I suggest not to mix different styles like chaotic vs. chaotical, dynamic vs. dynamical, $\dot{x}$ vs. $\frac{dx}{dt}$, $e = \eta - \hat{\eta}$ vs. $e = \hat{\eta} - \eta$, $\bar{\Theta} = |\Theta|$ vs. $\Theta = |\bar{\Theta}|$, $\tau_m$ vs $\tau_{mast}$, Lyapunov function vs. Lyapunov's function.
- I also suggest to pay more attention to grammar: was vs. were, end vs. and, robust vs robast, international vs. intarnational, is vs. are, has vs. have, can not vs. cannot, derivation vs. derivative.
- A list of symbols and abbreviations would be nice.

Final verdict: I suggest the thesis as fulfilling the requirements for the degree of Ph.D.
Prague, 30. June 2010

Pavel Pokorný