PhD Proposal 2017

School: Ecole Centrale de Nantes	
Laboratory: IRCCyN	**Web site: http://www.irccyn.ec-nantes.fr/**
Team: Control	**Head of the team: F.Plestan / Ph.Chevrel**
Supervisor: Ina Taralova	**Email: ina.taralova@irccyn.ec-nantes.fr**
Collaboration with other partner during this PhD: **In France:** • **IETR Laboratory in Rennes (Group on secure communications)** • **CNRS Laboratory J. A. Dieudonné, University of Nice - Sophia Antipolis**	**In China:**

Title: Nonlinear dynamics, applications to secure information transmission
Scientific field: Automation and robotics, applied mathematics
Key words: : Dynamical system, chaos, nonlinear control, bifurcation, encryption

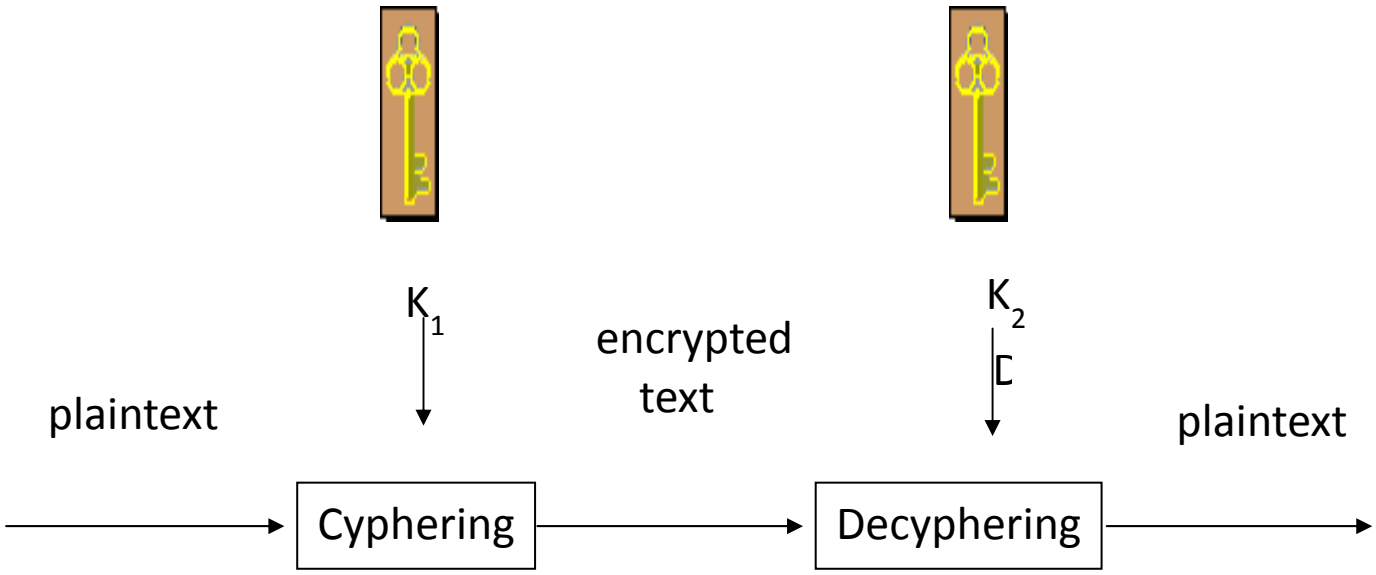
Details for the subject:

Background, Context:

Chaotic systems are defined by their extreme sensitivity to small variations in the initial conditions and parameters (known as the “butterfly effect”). It should be noted that chaotic behavior can be observed in basic nonlinear dynamical systems, such as the recurrence equation x(k+1) = x(k)^2 +c where chaos appears for some particular values of c.

In addition, complex (e.g. chaotic) behavior can be exhibited by some apparently simple systems - like the quadratic map above, but also some piece-wise linear (PWL) maps, etc. That simplicity makes them a priori attractive for different real-life applications such as Secure Communications, Information Encryption, or Secure Electronic Transactions. Besides, the PWL maps can be considered also as switched systems, and therefore, analyzed with the control theory tools.

In the figure below, the key K_1 (corresponds to the chaotic sequence) is used for the encryption of the plaintext. After that, the encrypted text is transmitted over the transmission channel. Finally at the receiver, the original plaintext is retrieved (decyphered) using the key K_2 (an identical chaotic sequence, or a nonlinear observer). Because of the increasing number of e-transactions, the necessity of generating large size encrytion keys is incessantly growing. For this aim, efficient Chaotic Pseudo-Random Number Generators (CPRNG) are expected to produce robust pseudo-random sequences, where small changes in the system parameters and initial parameters (i.e. the encryption key) would lead to essential qualitative modification of the encrypted information.



The main difficulties are due to the fact that well-known chaotic maps *are not naturally suitable* for encryption purposes when taken individually. Indeed, they don’t exhibit even minimal satisfactory properties for this application, mainly *because of their weak chaoticity*. A judicious coupling between these maps appears to be a good solution. Then, many open problems arise: the required structure for an efficient chaotic generator (e.g. the chaotic map), the criteria to analyze the control parameters, the choice of the best coupling between the PWL and other chaotic maps in order to satisfy the predefined criteria for strong chaoticity etc.

Research subject, work plan:

After a bibliographic search to analyze the current state of the art, this Ph.D. thesis will cope first with the global understanding and study of the nonlinear behavior of coupled chaotic systems, stability analysis, completed by the study of the bifurcations diagrams and the roads which lead to chaos.

Then, different kind of chaotic maps couplings (auto- and ring- couplings), inspired by electrical – and other - circuits, will be analyzed, in order to obtain the defined features for both chaotic, and pseudo-random /and therefore, repetitive/ behavior, required for decyphering. The system, when used in chaotic regime is expected to generate uncorrelated (independent) output signals. Under some conditions, the latter will be considered as pseudo-random sequences, and will be applied as chaotic pseudo-random carriers for secure information transmission.

The control theory concepts of identifiability and observability for switched systems will be applied in order to select the most suitable chaotic system. The latter will be applied as pseudo-random number generator, which may be used in various applications; here in particular for secure information transmission, and applications to cryptography. Nonlinear observers will be designed to synchronize the emitter (cyphering bloc) and the receiver (decyphering bloc). If the chaotic generator is *observable,* its parameters have to be known (or *identifiable*): they are used a as secret keys from information security point of view. Therefore, the system has to be verified for observability (i.e. the overall CPRNG dynamics can be analytically retrieved from its output signal). Another study shall be carried out concerning the range of all possible parameters for which these features can be preserved, with the aim to increase the size of the secret key, and therefore to improve the security.

Successful applicants should have good background in one of the following fields: applied mathematics, dynamical systems, signal processing, control theory, communications. Knowledge in DSP and Matlab/Simulink shall be greatly appreciated.

Collaborations:

During this PhD project, an active collaboration is being set up with S. El Assad from IETR Laboratory in Rennes (group on secure communications) and R. Lozi from the CNRS Laboratory J. A. Dieudonné, University of Nice -Sophia Antipolis.

References:

1. O. Garasym, I. Taralova, R. Lozi, "Robust PRNG based on homogeneously distributed chaotic dynamics", IoP *Journal of Physics* 2016 (to appear)

2. O. Garasym, I. Taralova, R. Lozi, "New nonlinear CPRNG based on tent and logistic maps", *Complex Systems and Networks - Dynamics, Controls and Applications*, 2015, Springer (book chapter) pp. 131-161.

3. O. Garasym, I. Taralova, R. Lozi, "Application of observer-based chaotic synchronization and identifiability to original CSK model for secure information transmission"*, Indian Journal of Industrial and Applied Mathematics*, 2015, Vol. 6, No. 1, pp. 1-35.

4. R. Lozi, I. Taralova, "From chaos to randomness via geometric undersampling", *European Series in Applied and Industrial Mathematics ESAIM: Proceedings and surveys,* 2014, Vol. 46, pp. 177-195.

5. G. Alvarez, S. Li, Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *International Journal of Bifurcation and Chaos (IJBC)*, Vol. 16, 2006, pp. 2129-2151.

6. I. Taralova, Chaotic orbits prediction and atypical bifurcations in a class of piece-wise linear noninvertible maps, *European Physical Journal - Special Topics*, Vol. 165, Issue 1, 2008, pp. 45–59.

7. R. Lozi, Designing Chaotic Mathematical Circuits for Solving Practical Problems, *International Journal of Automation and Computing* 11(6), 2014, pp.588-597.