Workshop « Analyse du chaos et applications »

Le vendredi 6 décembre 2019

À l'ENSEA (6 Avenue du Ponceau, 95000 Cergy), en salle A302 (bâtiment A, troisième étage).

10h00 - 10h30 : **Accueil des participants**

10h30 - 11h15 : **Une théorie symbolique nonlinéaire pour l'observabilité et la contrôlabilité des réseaux**
Christophe Letellier, Normandie Université CORIA

Lorsqu'un réseau complexe de N_n nœuds, chacun animés d'une dynamique de dimension d est étudié, l'un des objectifs est de récupérer la dynamique de l'ensemble du système par la mesure de quantités bien choisies au sein de nœuds également bien sélectionnés. Le choix des nœuds à mesurer (senseurs) est l'un des problèmes essentiels dans l'étude des réseaux puisque, trop souvent, leur dimensionnalité est trop grande pour permettre la mesure de l'ensemble des variables requises pour la détermination complète de tous les états du système.

Comme connaissance a priori, nous nous limitons à la matrice d'adjacence et aux équations gouvernant chaque nœud (nous pouvons montrer qu'il nous est possible de récupérer ces équations par une technique de modélisation globale). La procédure pour établir l'observabilité d'un réseau se décompose en quelques étapes comme suit. Premièrement, l'observabilité d'un nœud isolé est estimée. Ensuite, celle d'une paire de nœuds, est étudiée. Nous entreprenons de vérifier qu'un observateur peut effectivement être construit pour chacun de ces deux cas. La précision des observateurs est quantifiée dans ces deux cas. Typiquement, nous avons conjecturé qu'il n'était pas possible de reconstruire plus de deux nœuds à partir de mesures réalisées dans un seul nœud. Une fois ces deux étapes réalisées, il est alors possible de grouper les nœuds d'un réseau par paires, et de traiter ainsi un réseau de n'importe quelle dimension. A titre d'exemple pratique, nous considérerons une réseau aléatoire de $N_n = 28$ nœuds, constitué d'une dynamique de type Rössler, et pour laquelle nous avons une réalisation électronique.

Des résultats préliminaires sur la contrôlabilité symbolique seront également présentés.

Ce travail est réalisé avec Irène Sendina-Nadal (RJC University, Madrid) et Sylvain Mangiarotti (CESBIO, Toulouse).

References

[1] L. A. Aguirre & C. Letellier, Observability of multivariate differential embeddings, Journal of Physics A, 38, 6311 (2005).

[2] E. Bianco-Martinez, M. S. Baptista & C. Letellier, Symbolic computations of non-linear observability, Physical Review E, 91, 062912, 2015.

[3] C. Letellier, I. Sendiña-Nadal, E. Bianco-Martinez & M. S. Baptista, A symbolic network-based nonlinear theory for dynamical systems observability, Scientific Reports, 8, 3785, 2018.

[4] C. Letellier, I. Sendiña-Nadal & L. A. Aguirre, A nonlinear graph-based theory for dynamical network observability, Physical Review E, 98, 020303(R), 2018.

[5] I. Sendiña-Nadal & C. Letellier, Observability of dynamical networks from graphic and symbolic approaches, In Springer Proceedings in Complexity, X S. Cornelius, C. Granell Martorell, J. Gómez-Gardeñes & B. Gonçalves (eds) CompleNet 2019.

11h15 - 11h45 : **Constructing flat inputs for two-output systems and application to private communication**

Florentina Nicolau, Quartz, Ensea Cergy

We study the problem of constructing flat inputs for two-output dynamical systems. The notion of flat inputs has been introduced by Waldherr and Zeitz (2008, 2010) and can be seen as dual to that of flat outputs. In the single-output case, a flat input can be constructed if and only if the original dynamical system together with its output is observable. In the multi-output case, the observability is not necessary for the existence of flat inputs. The goal of this presentation is thus to treat the unobservable one and we will consider the case of two-output systems. We show that locally, on an open and dense subset, there always exist control vector fields g_1 and g_2 such that the associated control-affine system is flat with the original output being a flat output. Finally, we explain how our results can be applied to private communication.

Work in collaboration with : W. Respondek (LMI, INSA Rouen Normandie), J.P. Barbot and A. Ouslimani (Quartz, Ensea Cergy).

11h45 - 12h15 : **A digital receiver for an analog transmitter in a private communication scheme**

Octaviana Datcu, Politehnica University of Bucharest

One of the simplest jerk-type circuit manifesting chaotic behavior is considered as the transmitter in a communication scheme. A previous work has analyzed the observability properties when estimating its dynamics, given that only one of its states is transmitted over the communication channel. High order sliding-mode observers have, then, been implemented to this end. The present approach brings a new perspective in aligning to the analog circuitry, using Simscape components in Matlab-Simlink and wiring the circuit on the breadboard. The analog circuitry is sampled with an oscilloscope and the data series are saved in a .csv file. Then, the same sliding-mode observer is used to estimate the states of the transmitter in the two new scenarios. Its parameters are changed accordingly and differences between the these situations are concluded. The step presented by this paper is to be integrated in an analog transmitter-FPGA based sliding mode observer hybrid communication scheme. In a second step, a flat chaotic transmitter is studied using the same approach. Its usefulness when coupling an unobservable chaotic system with an observable one was proven in the literature from the theoretical point of view. The new perspective aims to highlight the physical aspects of such a construction.

12h15 - 13h30 : **Pause déjeuner**

13h30 - 14h15 : **Chaos-based Cryptography Primitives for Data Security : Encryption, Steganography, Hashing**

Safwan El Assad, IETR, Université de Nantes/Polytech Nantes

Compared to the “Classical Cryptography”, “Chaos-based Cryptography” and especially chaos-based encryption : stream cipher and block cipher have strong diffusion property and they are more modular (existence of a generic model), more flexible (block size, secret key size) and easier to be implemented, which make them more suitable for large scale-data encryption such as images and videos.

The heart of the chaos-based cryptography is the chaotic generator and so, a part of the performance (security, computational complexity) of the system depends greatly on it.

In this talk, we give an example of : Chaos-based stream cipher, Chaos-based block cipher, Chaos-based steganography system, Chaos-based hash function.

Work in collaboration with : Fethi Dridi, Guillaume Gautier, Nabil Abdoun, Olivier Deforges

References :

[1] S. El Assad, H. Noura, “Generator of chaotic sequences and corresponding generating system”, Patent EP 2553567 B1, US 8781116 B2

[2] M. Abutaha, S. El Assad, A. Queudet, O Deforges, “Design and Efficient Implementation of a Chaos-based Stream Cipher”, Int. J. Internet Technology and Secured Transactions, Vol. 7, No. 2, Sept 2017, pp.89–114.

[3] Jallouli, S. El Assad, M. Chetto, R. Lozi, “Design and Analysis of two Stream Ciphers Based on Chaotic Coupling and Multiplexing techniques” MTAP, Multimedia Tools and Applications, June 2017, pp. 1-27. DOI 10.1007/s11042-017-4953-x

[4] Farajallah, S. El Assad, O. Deforges, “Fast and secure chaos-based cryptosystem for images”, International Journal of Bifurcation and Chaos, IJBC, February 2016, Vol. 26, No. 02, pp. 1650021-1 1650021-21. DOI : 10.1142/S0218127416500218.

[5] D. Battikh, S. El Assad, T. M. Hoang, B. Bakhache, O. Deforges, M. Khalil,” Comparative Study of Three Steganographic Methods Using a Chaotic System and Their Universal Steganalysis Based on Three Feature Vectors”, Entropy 2019, 21, 748 ; doi :10.3390/e21080748, www.mdpi.com/journal/entropy.

[6] Abdoun, S. El Assad, O. Deforges, R. Assaf, M. Khalil,” Design and Security Analysis of Two Robust Keyed Hash Functions based on Chaotic Neural Networks”, AIHC-2019, Journal of Ambient Intelligence and Humanized Computing, February 2019, 25 pages https ://doi.org/10.1007/s12652-019-01244-y

14h15 - 14h45 : **A robust pseudo-chaotic number generator for cryptosystem based on chaotic maps and multiplexing mechanism**

Zongchao QIAO, LS2N, Ecole Centrale de Nantes

With the rapid development of new internet technology and communication network, huge amounts of various digital data, for instance text message, image, audio signal and video with confidential information are exchanged via insecure network channels, which require a good cryptosystem that can resist any kind of attacks to ensure the information security.

The cryptographic keys are crucial in cryptosystems. According to Kerckhoffs’ principle, the security of a cryptosystem should depend only on its key. Thus, they should have large key space and exhibit random properties to guarantee high security. Over the years, chaos-based Pseudo-Random Number Generators (PRNGs) have been verified to be efficient in producing pseudo-random numbers due to their excellent properties, such as, deterministic character, non-periodicity, high sensitivity to initial conditions and parameters, etc.

Here, we propose to design and analyze a new robust Pseudo-Chaotic Number Generator (PCNG) based on discrete chaotic maps over finite field and a multiplexing mechanism. The proposed PCNG contains three discrete chaotic maps : Piece-Wise Linear Chaotic Map (PWLCM), skew tent and logistic map. Three XOR operators are applied on these maps to form three optional intermediate outputs that are selected by the multiplexing mechanism to produce the final pseudo-chaotic sequence. The PCNG is designed over a finite 232 bits field with 2159 key space. The latter allows to palliate the problems of deteriorated security caused by the dynamical degradation (i.e. unexpected low period orbits or even fixed points, round-off errors, waste of computational time to convert reals to integers etc. related to the numerical implementation of real numbers chaotic maps. Thus, the proposed PCNG is more performant and secure for cryptography purposes. In addition, it has a simple structure and can be easily implemented.

Security analyses and statistical experiments, including key space and key sensitivity analyses as well as histogram, Chi-square and NIST tests, have been carried out and the results have proven that the proposed PCNG can generate effective pseudo-random numbers and exhibits good security properties with large secret key space and high key sensitivity. Therefore, the proposed PCNG can be successfully applied not only in any design of new stream ciphers, block ciphers or other cryptosystems, but also in other engineering applications requiring fast and secure pseudo-random number generators.

Keywords : discrete chaotic maps ; finite field ; pseudo-chaotic number generator ; multiplexing mechanism ; security analysis, secret key

Work in collaboration with : Ina Taralova (LS2N, Ecole Centrale de Nantes), Safwan El Assad (IETR, Université de Nantes/Polytech Nantes)

14h45 - 15h15 : **Effets de troncature dans le chaos déterministe**

Roger Tauleigne, Quartz, Ensea Cergy

A l'aide de l'emblématique parabole logistique $x_{n+1} = \lambda x_n(1 - x_n)$, on explore les causes du chaos déterministe. Nous commençons par réduire la précision du système de numération utilisé dans le calcul des itérations.

De seize décimales, on réduit l'expression des nombres à deux décimales. On constate que les solutions chaotiques deviennent périodiques, indépendamment de la valeur du paramètre de contrôle. La valeur des périodes est extrêmement petite comparer à la puissance lexicographique du système de numération. Moins évident, les périodicités apparaissent comme proportionnelle au nombre de décimales.

Lorsque la précision est maximale, l'histogramme d'une solution chaotique présente une étonnante coïncidence avec l'histogramme de la fonction sinus. Le chaos déterministe de cette récurrence distribue ses valeurs exactement comme la fonction la plus régulière que peut prendre un mouvement d'aller-retour, la fonction sinus. Cette fonction autant héritière du principe de moindre action que d'une brisure de symétrie évidente.

Enfin, certaines modifications de la récurrence conduisent à un histogramme plat. La récurrence obtenu est nettement mieux adaptée à produire des nombres pseudo aléatoires que la parabole logistique.

15h15 - 15h30 : **Pause café**

15h30 - 16h45 : **Specific Coupling of Chaotic Attractors to Produce New Chaotic Attractors**

Ali Pacha Adda, LACOSI, University of Science and Technology of Oran, Algeria

The basic idea of this work is to find a better way to couple different chaotic attractors, homogeneous type or heterogeneous type. We study the result of this coupling.

Different attractors have been tested ; the results obtained are very satisfactory.

Keywords. Hénon Attractor, De Jong Attractor, Sensitivity of Initial Conditions, Calcul of the Lyapunov exponent.

16h45 - 17h15 : **Cryptanalysis of a compressive sensing communication scheme**

Corina Macovei, Politehnica University of Bucharest

A communication scheme uses a chaotic logistic map to generate the matrix employed to simultaneously compress and encipher a private multimedia message. The result is statistically analyzed, from the legitimate user's point of view. The eavesdropper's perspective is presented by performing a known plain text attack utilizing statistical tools.The results are obtained using Matlab and Simulink. Conclusions and research perspectives are drawn.

Work in collaboration with : Adina-Elena Blaj, Octaviana Datcu, Radu Hobincu.