Le Chaos (mathématique) est-il un instrument de progrès pour la cryptographie ?

René Lozi, Professeur (émérite), Laboratoire de mathématiques J. A. Dieudonné, Université Côte d'Azur (Nice)

La cryptographie est une science dont les origines sont très lointaines, puisque qu'on connait la façon dont les Romains, au temps de Jules César codaient leurs messages militaires. Elle n'a cessé de progresser au fil de siècles : code de Vigenère en 1553, machine Enigma utilisée par les Allemands durant la seconde guerre mondiale, et plus récemment codage à clef publique (algorithme RSA, 1978). Depuis 50 ans, les mathématiques sont au cœur des recherches et des avancées en cryptographie. Plus récemment, une nouvelle branche de la cryptographie : la cryptographie basée sur le chaos mathématiques, se développe fortement.

La notion de chaos mathématique a été introduite en 1975 par Tien-Yen Li et James Yorke dans leur fameux article « period three implies chaos ». Depuis cette date, les recherches sur les systèmes dynamiques chaotiques et les attracteurs étranges ont beaucoup progressé, leurs applications en cryptographie aussi. Nous allons présenter les tendances actuelles de ces recherches, les difficultés qu'elles rencontrent, mais également leur succès, et les perspectives que l'on peut attendre d'elles.

Professeur René Lozi Curriculum vitae

Professor René Lozi

He was born in 1948 and received his Ph.D. in numerical analysis (bifurcation theory) from the University of Nice in 1975. In 1983, he received the French State Thesis from University of Nice under the supervision of Prof. René Thom (Fields medalist in 1958). He has been Assistant Professor, Laboratoire J. A. Dieudonné, University of Nice (1974-1976); Research Attaché of Centre National de la Recherche Scientifique (CNRS) (1976-1982), responsible for research at CNRS (1982-1990). He became Full Professor (2nd class) at Laboratoire J. A. Dieudonné, University of Nice and Institut Universitaire de Formation des Maîtres (IUFM), Nice (1990-2005). He has been Head of the Department of Mathematics, IUFM (1993-1997); President of the Scientific and Educational Board of IUFM (1993-1996); Director of the Institute of Research in the Teaching of Mathematics (IREM), University of Nice (1993-1997); Head of the Academic Mission of Teachers Training (MAFPEN) of the Southeast part of France Region Education Authority (1997-1998); Advisor for the new technologies of the Southeast part of France Region Education Authority (1998-1999). In 2005, he became Full Professor (1st Class) at Laboratoire J.A. Dieudonné, University of Nice and IUFM. He has served as the Director of IUFM (2001-2006) and as Vice-Chairman of the French Board of Directors of IUFM (2004-2006) and in 2011 he became Full Professor of Exceptional Class (the highest rank in French university). He is member of the Editorial Board of Indian Journal of Industrial and Applied Mathematics and Journal of Nonlinear Systems and Applications, and member of the Honorary Editorial Board of International Journal of Bifurcation and Chaos. He is life member of the Indian Society of Industrial and Applied Mathematics (and was there, when this society was established in Aligarh Muslim University, last week of September 1990). He his also member of the Interuniversity group of research DYCOEC, GdR 2984 of C.N.R.S. (Dynamics and control of complex sets), and the International Physics and Control Society (IPACS, St Petersburg, Russia).

His research areas include complexity and emergences theories, dynamical systems, bifurcation and chaos, control of chaos, cryptography based chaos, Genetic Algorithms, Evolutionary algorithms and recently Memristors. His initial research was related to the numerical analysis of the bifurcation phenomena in the fields of nonlinear boundary value problems of ordinary differential equations. Then he entered the domain of dynamical systems, in which in 1977 he discovered a particular mapping of the plane producing a very simple strange attractor (now known as the "Lozi map"). He has worked in this field with renowned researchers, such as Professors Leon Chua (inventor of "Chua circuit" and Memrsitor), and Alexander Sharkovsky (who introduced the "Sharkovsky's order"). He has been Visiting Professor for several short periods to the University of Kyoto and University of Tokushima in Japan, University of Berkley, USA, Universities of Hong-Kong and Shanghai, China. Some of his former students are now full Professors in the Universities of Le Havre, France; Constantine and Sétif, Algeria. His current research interest lies on one hand, in the use of dynamical systems in order to produce pseudo-random numbers in order to improve encryption methods or to enhance optization evolutionary algorithms, and on the other hand on Memristors (a new passive eletronic element which will revolutionize the industry of computers, in the coming few years). His currently working with a dozen of teams worldwide on those topics. In parallel with these strictly mathematical researches, he also studies several aspects of the teaching of mathematics in particular a new fields called interdidactics. With Professor Nicole Biagioli he has co-founded the interdisciplinary laboratory I3DL (InterDidactique, Didactique des Disciplines et des Langues) at the university of Nice-Sophia Antipolis.