Programme Journée Scientifique Fédération Charles Hermite

"Pseudorandomness, cryptography and number theory"

Date : Jeudi 9 décembre 2021
Lieu : LORIA, Amphithéâtre

8h30-9h00	Accueil

09h00-10h00 **Restrictions on Costas Arrays**
Domingo GÓMEZ-PÉREZ (Santander, Espagne)

Abstract : In 1965, J. P. Costas introduced a special class of permutations with applications to improving the target detection. The idea was to define a signal consisting of several frequencies transmitted at consecutive time intervals. Such a signal Is modeled as a binary matrix where rows are labelled with the different possible frequencies and the columns with the consecutive time intervals. Each column has only one element different from zero, representing the frequency of the signal at that time interval. The function that for each time interval returns the corresponding sequence is a permutation for the so called Costas arrays, which are the optimal solution for target detection when the number of frequencies and time intervals are equal.

It is customary to consider only square binary matrix and the optimal signals for target detection corresponds to matrices such that the number of coincidences between the original matrix and any non cyclic shifted version is always less than one.

In this talk we center on what happen when the shifted version of the matrix is done in a cyclic way. This quantity is called the deficiency of the Costas arrays and there are several conjectures made by Jedwab and Wodlinger and some relations with some structural properties found by Correll and other authors.

10h00-10h30 Pause-café

10h30-11h30 **New LFSRs and FCSRs matrix representations for stream ciphers hardware and software design**
Marine MINIER (LORIA)

Abstract : In this talk, we will sum up our research results concerning the introduction of a new matrix representation for FCSRs based upon a known LFSRs representation. This matrix based representation allows to construct FCSRs with a more compact hardware representation and a quicker diffusion while preserving the usual and proven good properties (good periods, l-sequences, good statistical behaviors, etc.). Moreover, this new approach circumvents the weaknesses of the Fibonacci and Galois representations. We also show how to extend the LFSRs representation to a particular LFSR case called the windmill case.

LFSRs are well-known primitives used in cryptography especially for stream cipher design. However they have some drawbacks when looking at their resistance against algebraic attacks because of their linearity. In the contrary, FCSRs are inherently resistant to algebraic attacks due to the non-linearity of the update function. Using the new representation, we propose two new stream ciphers based on the so-called ''ring'' FCSR representation. The first proposal called F-FCSR is dedicated to hardware applications whereas the second proposal called X-FCSR is designed for software purposes but is also efficient in hardware.

Organisateurs : Cécile DARTYGE (IECL) – cecile.dartyge@univ-lorraine.fr
Damien JAMET (LORIA) damien.jamet@loria.fr
Pierre POPOLI (IECL) – pierre.popoli@univ-lorraine.fr
Thomas STOLL (IECL) – thomas.stoll@univ-lorraine.fr

11h40-12h40 **Pseudo ness of the digits of primes**
Cathy SWAENEPOEL (IMJ, Paris)

Abstract : Are the digits of primes ''random'' ? Do they have properties similar to those of the digits of all natural numbers ? These general questions, not only interesting for primes but also for a lot of other sequences, are at the source of many challenging problems in number theory and have connections with cryptography.

In this talk, we will focus on the digits of primes which have attracted a lot of interest in recent years. To explore their pseudorandom properties, we will discuss some interesting results (including results by Mauduit-Rivat, Maynard, Bourgain and myself) providing estimates for the number of primes whose digits satisfy certain conditions.

12h40-14h30 Repas

14h30-15h30 **On bent functions: a selection of some achievements and open problems**
Sihem MESNAGER (Université de Paris VIII)

Abstract : Boolean functions, F_2 -valued functions defined over the finite field F_{2^n} of order 2^n, play a central role in the security of the pseudo-random generators of stream ciphers. As components of vectorial Boolean functions, they are also widely applied to block ciphers' design in cryptography (where they are used to create the so-called substitution boxes, or S-boxes, whose input and output are then both sequences of bits).

We shall mainly focus on one crucial cryptographic parameter for Boolean functions: nonlinearity. Bent functions are maximally nonlinear Boolean functions. They are important creatures introduced by O. Rothaus in the 1960s and initially studied by J. Dillon since 1974. They have attracted a lot of research for more than four decades, thanks to their interesting connections to several domains with applications in cryptography.

In this talk, we shall introduce bent functions, provide some insight into them, and discuss some problems (namely on exponential sums) to increase our knowledge (in particular in design) about the corpus of bent functions (including their important subclasses: hyper-bent functions).

15h30-16h00 Pause-café

16h00-17h00 **Pseudorandomness of automatic sequences**
László MÉRAI (RICAM, Linz, Autriche)

Abstract : Many automatic sequences, such as the Thue-Morse sequence or the Rudin-Shapiro sequence, have some desirable features of pseudorandomness such as a large linear complexity and a small well-distribution measure. However, they also have some disastrous properties in view of certain applications. For example, the majority of possible binary patterns never appears in automatic sequences and their correlation measure of order 2 is extremely large.

Certain subsequences, such as automatic sequences along squares, may keep the good properties of the original sequence but avoid the bad ones.

In this talk I survey recent results and open problems on pseudorandomness and non-randomness of automatic sequences and their subsequences.

Inscription gratuite et obligatoire ici avant le 19/11/21

Organisateurs : Cécile DARTYGE (IECL) – cecile.dartyge@univ-lorraine.fr
Damien JAMET (LORIA) damien.jamet@loria.fr
Pierre POPOLI (IECL) – pierre.popoli@univ-lorraine.fr
Thomas STOLL (IECL) – thomas.stoll@univ-lorraine.fr