CENTRO DE MATEMÁTICA UNIVERSIDADE DO PORTO

Seminar on Computational Mathematics

Hyper-bent and generalized hyper-bent functions

Sihem Mesnager
(Paris)

Abstract. Hyper-bent Boolean functions were introduced in 2001 by Youssef and Gong (and initially proposed by Golomb and Gong in 1999 as a component of S-boxes) to ensure the security of symmetric cryptosystems but no cryptographic attack has been identified till 2016. Hyper-bent functions have properties still stronger than the well-known bent functions which were already studied by Dillon and Rothaus more than four decades ago. Hyper-bent functions are very rare and whose classification is still elusive. Therefore, not only their characterization, but also their generation are challenging problems. In the context of filtered LFSRs, Canteaut and Rotella showed at the 2016 FSE conference that when considering fast correlation attacks, the relevant criterion should no longer be nonlinearity, but rather generalized nonlinearity. Indeed, they showed that if $f + Tr(\lambda x^k)$ (where "Tr" stands for the absolute trace function over F_{2^n}) is biased, then we can apply a fast correlation attack to recover x_0^k where x_0 denotes the initial state. If k is coprime to $2^n - 1$, then the attack recovers the initial state. Moreover, the case when k is not coprime to $2^n - 1$ also leads to another attack and a new criterion to evaluate the security of filtered LFSR. The new criterion given on filtered LFSRs has thus revived interest in the topic of hyperbent functions. In this talk, we shall give a complete survey on all what is known on hyper-bent Boolean functions. We will also present very recent results (2018) on hyper-bent functions in arbitrary characteristic as well as generalized hyper-bent functions

Friday, July 27th, 2018 **14:30** **Room M029, DMat-FCUP**

Sihem Mesnager received the Ph.D. degree in Mathematics from the University of Pierre et Marie Curie (Paris VI), Paris, France, in 2002 and the Habilitation to Direct Theses (HDR) in Mathematics from the University of Paris VIII, France, in 2012. Currently, she is an associate Professor in Mathematics at the University of Paris VIII (France) in the laboratory LAGA (Laboratory of Analysis, Geometry and Applications), University of Paris XIII and CNRS. She is also Professor adjoint to Telecom ParisTech (France), research group MIC2 in mathematics of the department INFERES, Telecom ParisTech. Her research interests include discrete mathematics, symmetric cryptography coding theory, commutative algebra and computational algebraic geometry. She is Editor in Chief of the International Journal of Information and Coding Theory (IJOCT) published by Inderscience and co-Editor in Chief of the international journal Advances in Mathematics of Communications (AMC) published by AIMS. She is an Associate Editor for the international journal IEEE Transactions on information Theory (IEEE-IT) and also serves the editorial board of the international journal Cryptography and Communications Discrete Structures, Boolean Functions and Sequences (CCDS) published by SPRINGER and the international journal RAIRO ITA (Theoretical Informatics and Applications). She was a program co-chair for three International Workshops and served on the board of program comitties of fifteen international conferences and workshops. Since 2016, she is president of the french Chapter of IEEE in information theory. Since 2017, she is the head of the research team MTII "Mathematics for information and image processing" in the laboratory LAGA. (`https://www.math.univ-paris13.fr/ mesnager/index-en.html`)

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

QUADRO DE REFERÊNCIA ESTRATÉGICO NACIONAL PORTUGAL 2007-2013
GOVERNO DA REPÚBLICA PORTUGUESA
UNIÃO EUROPEIA Fundo Social Europeu

Com o apoio do projeto UID/MAT/00144/2013