On bentness and the nonlinearity of vectorial Boolean functions

Sihem Mesnager
(joint work with Claude Carlet, Chuankun Wu and Yuwei Xu)

LAGA and University of Paris VIII

Maximally nonlinear (n, m)-functions (the so-called bent vectorial functions) contribute to an optimal resistance to both linear and differential attacks on symmetric cryptosystems. They can be used in block ciphers at the cost of additional diffusion/compression/expansion layers, or as building blocks for the construction of substitution boxes (S-boxes) and they are also useful for constructing robust codes and algebraic manipulation detection codes.

Firstly, we study monomial functions $Tr_m^n(\lambda x^d)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, where m is a divisor of n. We establish several results leading to the classification of those bent monomials. Next, we study vectorial functions with multiple trace terms involving general results. Notably, we investigate some open problems raised by Pasalic et *al* and Muratović-Ribić et *al* and find new families of bent vectorial functions.

Secondly, we study the nonlinearity of (n, m)-functions. No tight upper bound is known when $\frac{n}{2} < m < n$. The covering radius bound is the only known upper bound in this range (the Sidelnikov-Chabaud-Vaudenay bound coincides with it when $m = n - 1$ and does not give any information when $m < n-1$). Finding better bounds is an open problem since the 90's. Moreover, no bound has been found during the last two decades which improve upon the covering radius bound for a large part of (n, m)-functions. We establish new upper bounds for functions which are unbalanced and improve a previous bound established by Carlet and Ding. These upper bounds imply necessary conditions on vectorial functions to have large nonlinearity.