SIHEM MESNAGER, University of Paris 8, Paris 13 and Telecom ParisTech
Recent advances on bent functions for symmetric cryptography

Boolean functions are important objects in discrete mathematics. They play a role in mathematics and in many domains of computer science. We will be mainly interested in their relationships with private-key cryptography.

The talk is devoted to special families of Boolean functions which are viewed as important objects in combinatorics and the information theory framework (namely, cryptography and coding theory) : the so-called bent functions.

Bent functions are maximally nonlinear Boolean functions. They are wonderful creatures introduced by O. Rothaus in the 1960's and initially studied by J. Dillon since 1974. For their own sake as interesting combinatorial objects, but also for their relations to coding theory (e.g. Reed-Muller codes, Kerdock codes, etc.), combinatorics (e.g. difference sets), design theory, sequence theory, and applications in cryptography (design of stream ciphers and of S-boxes for block ciphers), they have attracted a lot of research for four decades.

We give a survey of the main results in bent functions and present new ones.