PETR LISONEK, Simon Fraser University, Burnaby, BC
Bent functions on finite fields

Bent functions are a class of functions from $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ that are in a precise sense as far as possible from any affine function. This makes them resistant to some well-known cryptographic attacks. There are other features desired in the cryptographic applications, such as a high algebraic degree of the function, and the talk focuses on classes of bent functions that perform well with respect to such additional criteria.

We show how tools from different areas, such as arithmetic geometry (elliptic and hyperelliptic curves), finite fields (character sums) and combinatorics (spreads, relative difference sets, Desarguesian planes) are all used in the study of bent functions. The results are theoretical (characterizations, necessary conditions, constructions) and algorithmic (polynomial time certification of bentness).