ALPEN-ADRIA UNIVERSITÄT KLAGENFURT

INVITATION TO THE DOCTORAL SEMINAR

Cryptographic functions, bent functions and partitions

Wilfried Meidl | Radon Institute for Computational and Applied Mathematics, OEAW, Linz

Chaired by Clemens Heuberger | Department of Mathematics

Wednesday, 24 February 2021 | 10:00–11:00

https://classroom.aau.at/math-stat

ABSTRACT

In the first part, cryptographic functions like (vectorial) bent functions, almost bent functions, APN-functions are introduced. and connections to coding theory, objects from combinatoric and finite geometry are highlighted.

In the second part, the construction of bent functions from spreads of $\mathbb{V}_n^{(p)}$, $n = 2m$, is explained, where $\mathbb{V}_n^{(p)}$ denotes an n-dimensional vector space over a prime field $\mathbb{F}_p$. A construction of bent functions from $\mathbb{V}_n^{(2)}$ into $B(2^k)$, where $B(2^k)$ can be any abelian group of order 2^k, $k \leq n/6$, is presented. This construction, the first known construction different from the spread construction that is applicable for arbitrary abelian groups $B(2^k)$, is obtained from partitions of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, which can be seen as generalizations of the Desarguesian spread.

We hope to see you there!