Einladung

zum Vortrag im Rahmen des **SFB Colloquiums** (Standort Linz), mit dem Titel

Cyclotomic Cosets and Affine Equivalences Count in Prime Dimensions

VORTRAGENDER: **Pante Stanica**, Naval Postgraduate School
DATUM: Mittwoch, 27. Mai 2015
ZEIT: 10:15 Uhr
ORT: Science Park 2, S2 416-2, JKU Linz

Abstract:
A Boolean function is a map from the n-dimensional vector space $\mathbb{F}_2^n$ with values in the two-element field $\mathbb{F}_2$. They are extensively used as combiners in stream ciphers, as well as some other cryptographic settings.
A Boolean function is called *rotation symmetric* if its algebraic normal form (polynomial representation) is invariant under a cyclic permutations of indices. A monomial rotation symmetric function (MRS) of degree d is a rotation symmetric function generated by a single monomial $x_1x_{j_2}x_{j_3}\dots x_{j_d}$, that is, $f(x_1,\dots,x_n) = x_1x_{j_2}x_{j_3}\dots x_{j_d} + x_2x_{j_2+1}x_{j_3+1}\dots x_{j_d+1}+\dots$, where indices are taken Mod n (a Mod n is the unique integer $1 \le b \le n$ with $b \equiv a \pmod n$).
There are many papers dealing with the following (related) questions:

(A) Given two multivariable functions f, g, does there exist a permutation σ on the variables such that $f \circ \sigma = g$?

(B) How many classes of (such) equivalent functions are there?

These questions are relevant for cryptography, since if all "things" are equal, then one might want to use in a stream cipher an easier representable function from the same equivalence class. Using a new method previously developed by the author, D. Canright and J.H. Chung, we are able to completely count the number of equivalence classes for MRS of degree three, four and five in prime power dimension, as well as give "exact" asymptotics for arbitrary degrees. Most of the lecture will be accessible to a general mathematical audience.

Das **SFB Colloquium** wird vom **FWF Special Research Program (SFB) Quasi-Monte Carlo Methods: Theory and Application** unterstützt