Seminar Announcement

Speaker: Oğuz Yayla
Atılım University
Department of Mathematics

A better estimate on the number of non-empty intersection of 'boxes' of a finite field and its applications to pseudorandom sequences

Abstract

We improve an essential step of the estimation of the pseudorandomness of several sequences generated via additive order over a finite field. We give a better estimate on the number of non-empty intersection of `boxes' of a finite field. Then we apply this result to several sequences on the area of pseudorandom sequences: the general lattice test for the inversive and the nonlinear pseudorandom number generators, the correlation measure of digital explicit inversive pseudorandom numbers and the bound on their linear complexity profile, the correlation measure of binary sequences of quadratic characters of finite fields.

DATE: December 17, 2014
TIME: 15:30
PLACE: FEF 404 (Seminar Room)

All interested people are cordially invited.
After the seminar, some cookies and soft drinks will be served.