



Algebra and Number Theory Seminar

Title: On a class of bent functions

Speaker: Petr Lisonek (Simon Fraser University)

Date: Wed 16th June 2010 at 12:00PM

Location: Mathematical Sciences Seminar Room

Abstract: We look at the class of monomial and multinomial bent functions on $GF(p^{2m})$ for which each exponent in their trace representation is divisible by $p^m - 1$. The study of these functions is related to the theory of finite fields and their applications in cryptography and coding theory.