UCD School of Mathematics and Statistics

University College Dublin
Belfield, Dublin 4, Ireland

Tel +353 1 716 2580
Fax +353 1 716 1196

Scoil na Matamaitice agus na Staitisticí UCD

An Coláiste Ollscoile, Baile Átha Cliath
Belfield, Baile Átha Cliath 4, Éire

Email seminars@maths.ucd.ie
Web maths.ucd.ie/seminars

Algebra and Number Theory Seminar

Eimear Byrne (UCD)

will speak on

CCZ-Equivalence and Codes

Mon 1st February 2010 at 4:00PM

Location: Mathematical Sciences Seminar Room

CCZ-Equivalence is a topic normally studied in relation to APN functions. A pair of functions that are CCZ-equivalent have the same resistance to differential and linear cryptanalysis. It can be quite difficult to establish inequivalence of functions, even for power functions. A conjecture of Edel states that a pair of quadratic functions are CCZ-equivalent if and only if they are extended affine (EA)-equivalent. In this talk we discuss recent progress on this problem, with an application to the Gold functions. Theses results use some knowledge of the automorphism group of a binary code associated with a quadratic function.

This talk is part of the **Algebra and Number Theory** series. For more, see
https://maths.ucd.ie/seminars