Algebra and Number Theory Seminar

Title: CCZ-Equivalence and Codes

Speaker: Eimear Byrne (UCD)

Date: Mon 1st February 2010 at 4:00PM

Location: Mathematical Sciences Seminar Room

Abstract: 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.