Algebra and Number Theory Seminar

Title: Error-correcting Codes using Matrices for Post-Quantum Cryptography

Speaker: John Sheeky (UCD)

Date: Thu 13th February 2020 at 2:00PM

Location: Seminar Room SCN 1.25

Abstract: Error-correcting Codes have long been used to enable the reliable and efficient communication or storage of information in the presence of errors/noise. In 1978, McEliece proposed the use of error-correcting codes in cryptography; that is, for the secure and efficient communication of information. At the time, this scheme compared poorly with competitors in some respects, and so did not catch on in practice.

However, the hypothetical future existence of a large quantum computer would render most of the commonly used cryptographic systems insecure. This has led to a drive to develop, analyse, and standardise cryptosystems for which there is no known quantum algorithm to attack it. McEliece-type cryptosystems are one such family. Variants of this system using different metrics have been proposed for the ongoing NIST competition for Post-Quantum Cryptography.

We will present an idea which used rank-metric codes; codes where the codewords are matrices, and the distance between two matrices is the rank of their difference. We will discuss the strengths and weaknesses of these codes in general, and propose

a new implementation which (hopefully) retains their strengths and eliminates their weaknesses. This is a work in progress.

https://calendar.google.com/calendar/r/agenda/2019/1/20?tab=cc