K-Theory, Quadratic Forms and Number Theory Seminar

Title: Breaking RSA Encryption with a Quantum Computer: Shor's Factoring Algorithm

Speaker: Dr Colin Wilmott (UCD)

Date: Wed 6th December 2006 at 4:00PM

Location: Mathematical Sciences Teaching Room

Abstract: Arguably the most spectacular breakthrough in quantum computation was achieved when Shor presented a quantum algorithm for factoring an n-bit integer. This is a task which is believed to be intractable on a classical computer. I will discuss the means by which Shor's algorithm provides an expontential speed-up over the best known classical algorithm for factoring.

This is a joint Number Theory/Claude Shannon Institute seminar.