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

K-Theory, Quadratic Forms and Number Theory Seminar

Dr Colin Wilmott (UCD)

will speak on

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

Wed 6th December 2006 at 4:00PM

Location: Mathematical Sciences Teaching Room

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.

This talk is part of the **K-Theory, Quadratic Forms and Number Theory** series. For more, see
`https://maths.ucd.ie/seminars`