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

Steven Galbraith (Royal Hollaway, University of London)

will speak on

Point Compression and Multiplication for Pairing Based Cryptography

Wed 23rd April 2008 at 4:00PM

Location: Mathematical Sciences Seminar Room

Please note day and time The topic of this talk is elliptic curve cryptography.

I will discuss elliptic curve point compression in the context of pairing based cryptography. I will also present a method to speed up point multiplication in pairing friendly groups.

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