“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Ciaran Mullan

(Royal Holloway, University of London)

"Cryptanalysis of two matrix-based key establishment protocols ."

Feb 16, 12:00am (New York Time).

Abstract:

In this talk we will discuss two recent key establishment protocols. The first is due to Baumslag, Camps, Fine, Rosenberger and Xu (2006), and the second due to Habeeb, Kahrobaei and Shpilrain (2010).

For the first scheme, we offer a cryptanalysis when the platform group is SL_4(Z). And we cryptanalyze the second scheme when GL_n(F_p) is used as a platform.

For both schemes we will see some effective linear algebra tricks to efficiently derive the key, assuming only the passive adversary model.

Joint work with S.R. Blackburn and C. Cid.

Next presentation: **Mar 2, 2011.** Trapdoors for Lattices: Signatures, Identity-Based Encryption, and Beyond
Chris Peikert *(Georgia Institute of Technology)*

Algebraic Cryptography Center