“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

Simon R. Blackburn

(Royal Holloway, University of London)

“Searching for a secure Public Key Cryptosystem.”

Sep 20, 12:00pm (New York Time).

Abstract:

This talk will (mainly) be a tutorial on the development of our understanding of the security of public key cryptosystems, with an emphasis on some of the topics that are missed from many introductory cryptography textbooks for the pure mathematician. HIghlights will be:
- some (well-known) attacks on RSA, which imply that RSA as presented in introductory maths textbooks is insecure in practice;
- precise and stringent security definitions (as a reaction to these attacks);
- modifications to the basic RSA scheme that become secure (in the sense that they meet these security definitions under certain clear assumptions; and also in the sense that a careful implementation of the modified scheme is not broken in practice);
- some implications for group-based cryptography, including a critique of the security proofs in the textbook version of the Osin--Shpilrain scheme.

Next presentation: **TBA**

Algebraic Cryptography Center