February 28, 2002

Dan Boneh, Stanford University

Fast variants of the RSA cryptosystem

The RSA system is the most widely deployed public key cryptosystem. In this talk we survey four fast variants of RSA that are fully backwards compatible - a system using any of these variants can interact with a system using standard RSA. The design and cryptanalysis of these RSA variants is based on a number of algebraic techniques. The talk will be self-contained and describe some of the necessary algebraic tools.