"Symbolic Computations and Post-Quantum Cryptography" Online Seminar

Jintai Ding (University of Cincinnati)

"Post-quantum cryptography - multivariate public key cryptography ."

Feb 2, 12:00am (New York Time).

Abstract:

Quantum computer in theory can break all the currently used public key cryptosystems such as RSA and ECC. Post-quantum cryptosystems are public key cryptosystems that have the potential to resist the future quantum computee attacks. The focus of the talk will be multivariate public key cryptosystems, whose public keys are sets of multivariate polynomials over a small finite field.

Next presentation: **Feb 16, 2011.** *Matrix-based key agreement protocols: a cryptanalysis.*
Ciaran Mullan *(Royal Holloway, University of London)*

Algebraic Cryptography Center