Hide-and-Seek with Quadratic Forms and Finite Field Isomorphisms

Joseph Silverman, Brown University Mathematics Department

Cryptographic primitives such as public key cryptosystems and digital signature schemes rely on mathematical functions that are easy to compute, hard to invert in general, but possessing a ``trap-door'' that allows the function to be inverted easily if one has some additional information. In this talk I will discuss computational problems centered around quadratic forms and finite fields, which are interesting in their own right and which might be useful for constructing cryptographic primitives. (Joint work with J. Hoffstein, and in part with Y. Dor\"oz, J. Pipher, B Sunar, W. Whyte, Z. Zhang)