İTÜ Matematik Seminerleri

Complex Multiplication and Cryptographic Applications

Osmanbey Uzunkol

TÜBİTAK BİLGEM UEKAE, Mathematical and Computational Sciences Labs

Abstract

Complex multiplication combines the three Gaussian A's (Algebra, Analysis and Arithmetic) by means of a beautiful interplay between the geometry of abelian varieties with complex multiplication and the arithmetic of corresponding CM number fields. It has become subject to algorithmic investigations with different applications to algorithmic algebraic number theory and cryptography ranging from primality proving, elliptic curve cryptography, group- and pairing-based cryptography to the recent privacy enhancing techniques in cloud computation security.

In this talk, we give a survey of algorithmic and cryptographic aspects of complex multiplication together with some new results and some open problems.

Tarih: 5 Aralık 2014, Cuma

Saat: 15:15

Yer: Matematik Bölümü, B-326