

Abstract

Computational number theory is a new interdisciplinary subject, combining with number theory, computing theory, quantum computing, and cryptography, to name just a few. In this talk, I shall present some recent progress and new developments in computational number theory and number-theoretic cryptography, with an emphasis on new ideas in integer factorization and in breaking the RSA cryptography.