

Talk Title: Classical and quantum algorithms for problems from number theory

Abstract: Public-key cryptosystems are generally based on some well-studied mathematical problem, and the security of the system is related to the hardness of the underlying problem.

In this talk we will discuss recent classical and quantum algorithms for various problems from number theory used in public-key cryptography that are (or were) believed to be hard.