CC-07-02

Computationally hard problems for post-quantum cryptography

Yusuke Aikawa

The University of Tokyo

Abstract

The security of currently used public key cryptography is based on the computational hardness of problems such as the factorization problem and the discrete logarithm problem of groups. However, as is well known, these problems can be efficiently solved using Shor's algorithm, which has led to ongoing research and standardization efforts for cryptography that is resistant to cryptanalysis using both classical and quantum computers. Such cryptographic schemes are collectively referred to as post-quantum cryptography (PQC for short).

In this talk, we would like to share an overview of the types of PQC and the current trends in standardization. Additionally, we will discuss some of mathematical hardness assumptions underlying PQC, along with an evaluation of their hardness, incorporating our recent results.