Abstract:

Ring-LWE problem has been an important tool in cryptography to construct cryptosystems, key exchange protocols and homomorphic encryption schemes, which are expected to be secure against attacks by quantum computers. Cyclotomic fields are always used as underlying number fields of Ring-LWE problem from the viewpoints of security and efficiency. However, especially, in the case of homomorphic encryption schemes, improving the efficiency is still required.

Arita and Handa proposed to use certain subfields of cyclotomic fields with prime conductors, called decomposition fields, as underlying number fields of Ring-LWE problem to construct a homomorphic encryption scheme at ICISC 2017. Their homomorphic encryption scheme can provide many plaintext slots in which homomorphic arithmetics are easily executed. However, Arita et al. did not analyze the security of Ring-LWE problem over decomposition fields.

In this talk, we will present experimental results on attacks using lattices and ring structures against Ring-LWE problem over cyclotomic fields (with prime conductors) and decomposition fields, which indicate that Arita et al.'s homomorphic encryption scheme would be as secure as previous ones. This is a joint work with Shota Terada, Hideto Nakano and Atsuko Miyaji (Osaka University).