Cyclo-multiquadratic fields: fast polynomial arithmetic and homomorphic encryption

Iván Blanco Chacón (University of Alcalá - Madrid)

Abstract: In this talk we discuss cyclo-multiquadratic number fields, which are extensions of cyclotomic fields by quadratic roots of certain primes. In recent joint work with Pedrouzo-Ulloa, Barbero and Njah, we have introduced these fields to obtain a homomorphic encryption scheme which offers a reasonable theoretical security while keeping the complexity provided by the Number Theoretical Transform (NTT). In particular, the Polynomial Learning with Errors (PLWE) and Ring Learning with Errors (RLWE) problems are equivalent for this family of field and swapping between NTT and coefficient representations can be achieved at least twice faster than for the usual cyclotomic family. We will sketch these facts and discuss our ongoing research.