Code-based cryptography and AG codes

Alex Pellegrini
Eindhoven University of Technology

Abstract

Code-based cryptosystems rely on the hard problem of decoding a random linear code. Classic McEliece is an example of this family of cryptosystems and is taken in consideration for the fourth round of NIST standardization effort. The main drawback of McElice relies on the large public key size. In this talk, I will consider a version of McEliece using AG codes, surveying existing results and commenting on new work impacting performances and public key size.