

Speaker: Elena Kirshanova

Title: Construction-D lattice from Garcia-Stichtenoth tower code

Abstract. In this talk I present various existing constructions of lattices from codes. In particular, I present show an explicit construction of an efficiently decodable family of n -dimensional lattices whose minimum distances achieve $\Omega(\sqrt{n}/(\log n)^{\varepsilon+o(1)})$ for $\varepsilon > 0$. It improves upon the state-of-the-art construction due to Mook-Peikert that provides lattices with minimum distances $\Omega(\sqrt{n/\log n})$. These lattices are construction-D lattices built from a sequence of BCH codes. We show that replacing BCH codes with subfield subcodes of Garcia-Stichtenoth tower codes leads to a better minimum distance. To argue on decodability of the construction, we adapt soft-decision decoding techniques of Koetter-Vardy to algebraic-geometric codes.