Constructing genus 3 hyperelliptic Jacobians with CM: a cryptographer's point of view

Sorina Ionica, Ecole Normale Superieure

Isogeny graphs are graphs whose vertices are principally polarised abelian varieties with CM and edges are isogenies betweens these varieties. In dimension 3, the vertices of this graph arise as either Jacobians of hyperelliptic curves or Jacobians of plane quartic curves. Describing the structure of this graph is deeply related to answering the following question: given a sextic CM field K, are there any hyperelliptic Jacobians with CM by K? We revisit the construction in Vincent's talk and show effective computations of genus 3 hyperelliptic curves with CM. From a cryptographic point of view, we further evaluate the security of this construction, via attacks using isogeny graphs. This is joint work with J. Balakrishnan, K. Lauter and C. Vincent.