Class invariants for abelian surfaces

Andreas Enge
INRIA Bordeaux-Sud-Ouest, France
andreas.enge@inria.fr

Abelian surfaces, or equivalently Jacobians of genus 2 hyperelliptic curves, are the "next complex" case of abelian varieties after elliptic curves, and a serious contender for fast implementations of cryptosystems based on the discrete logarithm problem. Complex multiplication provides an interesting way of obtaining such surfaces with a known number of points over a finite field; it requires the costly computation of a large polynomial defining a certain class field.
I will report on joint work with Emmanuel Thomé on an asymptotically quasi-linear algorithm to compute such class polynomials with floating point approximations, as well as on its freely available implementation. Then I will present joint work with Marco Streng on a systematic approach for obtaining class invariants, that is, elements of the same class field with smaller minimal polynomials, and show how to solve the problem of obtaining all their algebraic conjugates in an easy way.

Joint work with Emmanuel Thomé (INRIA Nancy-Grand Est, France) and Marco Streng (Universiteit Leiden, Netherlands).