

ATELIER « COMPTAGE DE POINTS : THÉORIE, ALGORITHMES ET PRATIQUE »
19–23 AVRIL 2010

WORKSHOP ON COUNTING POINTS: THEORY, ALGORITHMS AND PRACTICE
APRIL 19–23, 2010

Families of curves amenable to RM-accelerated point counting

Benjamin Smith

Laboratoire d'Informatique (LIX)
INRIA Saclay - Île-de-France
École polytechnique
Route de Saclay, Palaiseau 91128
FRANCE

smith@lix.polytechnique.fr

In work in progress with Pierrick Gaudry and David Kohel, we use explicit Real Multiplication on Jacobians of genus 2 curves to accelerate Schoof's point counting algorithm.

In this talk, we will exhibit some two-parameter families of hyperelliptic curves with explicit Real Multiplication, following the approach of Mestre. These curves are amenable to our accelerated version of Schoof's algorithm, and have been used in some record-breaking point counting computations.