

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

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

Constructing genus 2 curves with a given number of points

Kristin Lauter

Cryptography Group
Microsoft Research
One Microsoft Way
Redmond, WA 98052
USA

klauter@microsoft.com

Genus 2 curves are useful in cryptography for both discrete-log based and pairing-based systems, but a method is required to compute genus 2 curves over finite fields such that the Jacobian has a given number of points. One approach involves constructing genus 2 curves with complex multiplication via computing their 3 Igusa class polynomials. These polynomials have rational coefficients and require extensive computation and precision to compute. Both the computation and the complexity analysis of these algorithms can be improved by a more precise understanding of the denominators of the coefficients of the polynomials. This talk will present new work which gives a bound on the denominators of Igusa class polynomials of genus 2 curves with CM by a primitive quartic CM field K .

This is joint work with Eyal Goren, McGill University.