1035-11-1352 **David Freeman*** (dfreeman@math.berkeley.edu), Department of Mathematics, University of California at Berkeley, Berkeley, CA 94720-3840, and **Kristin Lauter**, Microsoft Research, One Microsoft Way, Redmond, WA 98052. *Implementing the Genus 2 CM Method.*

In cryptography one often wishes to construct curves over finite fields whose Jacobians have a specified number of points. The best known technique for constructing such curves is the complex multiplication (CM) method. In the case of genus 2 curves, the method relies on computing Igusa class polynomials for quartic CM fields. There are three different approaches: a complex-analytic algorithm, a Chinese Remainder Theorem (CRT) algorithm, and a p-adic algorithm. These algorithms are less extensively developed than their elliptic curve analogues, and to date there is no running time analysis for any of them.

We will discuss two aspects of the genus 2 CM method: efficiently implementing Eisenträger and Lauter's CRT algorithm and estimating the running times of all three approaches. Efficiently implementing the CRT approach requires computing endomorphism rings of Jacobians of genus 2 curves over small finite fields; we have developed efficient algorithms to carry out this task. Estimating the running times requires bounding the coefficients of the Igusa class polynomials in terms of the discriminant of the quartic CM field; this is done by bounding the values of Siegel modular functions at CM points. (Received September 20, 2007)