Cryptology ePrint Archive: Report 2011/295

Counting Points on Genus 2 Curves with Real Multiplication

P. Gaudry and D. Kohel and B. Smith

Abstract: We present an accelerated Schoof-type point-counting algorithm for curves of genus 2 equipped with an efficiently computable real multiplication endomorphism. Our new algorithm reduces the complexity of genus 2 point counting over a finite field $GF(q)$ of large characteristic from $\sO(\log^8 q)$ to $\sO(\log^5 q)$. Using our algorithm we compute a 256-bit prime-order Jacobian, suitable for cryptographic applications, and also the order of a 1024-bit Jacobian.

Category / Keywords:

Date: received 3 Jun 2011

Contact author: pierrick gaudry at loria fr