Cryptology ePrint Archive: Report 2011/042

Computing endomorphism rings of elliptic curves under the GRH

Gaetan Bisson

Abstract: We design a probabilistic algorithm for computing endomorphism rings of ordinary elliptic curves defined over finite fields that we prove has a subexponential runtime in the size of the base field, assuming solely the generalized Riemann hypothesis.

Additionally, we improve the asymptotic complexity of previously known, heuristic, subexponential methods by describing a faster isogeny-computing routine.

Category / Keywords: foundations / endomorphism rings, GRH

Date: received 22 Jan 2011, last revised 14 Feb 2011

Contact author: gaetan bisson at loria fr

Available formats: PDF | BibTeX Citation

Version: 20110214:144107 (All versions of this report)