Cryptology ePrint Archive: Report 2011/143

Computing (ℓ,ℓ)-isogenies in polynomial time on Jacobians of genus~2 curves

Romain Cosset and Damien Robert

Abstract: In this paper, we compute ℓ-isogenies between abelian varieties over a field of characteristic different from 2 in polynomial time in ℓ, when ℓ is an odd prime which is coprime to the characteristic. We use level~n symmetric theta structure where $n=2$ or $n=4$. In a second part of this paper we explain how to convert between Mumford coordinates of Jacobians of genus~2 hyperelliptic curves to theta coordinates of level~2 or 4. Combined with the preceding algorithm, this gives a method to compute (ℓ,ℓ)-isogenies in polynomial time on Jacobians of genus~2 curves.

Category / Keywords: public-key cryptography / elliptic curve cryptosystem

Date: received 22 Mar 2011

Contact author: damien robert at inria fr

Available formats: PDF | BibTeX Citation

Version: 20110327:122130 (All versions of this report)

Discussion forum: Show discussion | Start new discussion