

All papers

(Help | Advanced search)

6

Go!

arXiv.org > math > arXiv:1204.0222

Mathematics > Number Theory

## Pairing-based algorithms for jacobians of genus 2 curves with maximal endomorphism ring

Sorina Ionica (INRIA Nancy - Grand Est / LORIA)

(Submitted on 29 Mar 2012)

Using Galois cohomology, Schmoyer characterizes cryptographic non-trivial self-pairings of the \$\ell\$-Tate pairing in terms of the action of the Frobenius on the \$\ell\$-torsion of the Jacobian of a genus 2 curve. We apply similar techniques to study the non-degeneracy of the \$\ell\$-Tate pairing restrained to subgroups of the \$\ell\$-torsion which are maximal isotropic with respect to the Weil pairing. First, we deduce a criterion to verify whether the jacobian of a genus 2 curve has maximal endomorphism ring. Secondly, we derive a method to construct horizontal \$(\ell,\ell)\$-isogenies starting from a jacobian with maximal endomorphism ring.

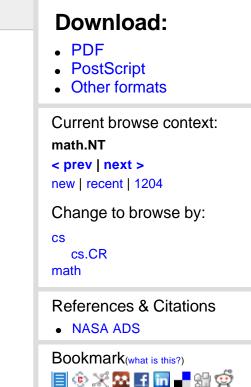
Subjects: Number Theory (math.NT); Cryptography and Security (cs.CR) Cite as: arXiv:1204.0222v1 [math.NT]

## **Submission history**

From: Sorina Ionica [view email] [v1] Thu, 29 Mar 2012 07:48:08 GMT (28kb)

Which authors of this paper are endorsers?

Link back to: arXiv, form interface, contact.



Science WISE

Search or Article-id