Cryptology ePrint Archive: Report 2013/192

A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties

David Lubicz and Damien Robert

Abstract: In this paper, we use the theory of theta functions to generalize to all abelian varieties the usual Miller's algorithm to compute a function associated to a principal divisor. We also explain how to use the Frobenius morphism on abelian varieties defined over a finite field in order to shorten the loop of the Weil and Tate pairings algorithms. This extend preceding results about ate and twisted ate pairings to all abelian varieties. Then building upon the two preceding ingredients, we obtain a variant of optimal pairings on abelian varieties. Finally, by introducing new addition formulas, we explain how to compute optimal pairings on Kummer varieties. We compare in term of performance the resulting algorithms to the algorithms already known in the genus one and two case.

Category / Keywords: foundations / Pairings, Abelian varieties

Date: received 2 Apr 2013

Contact author: damien robert at inria fr

Available formats: PDF | BibTeX Citation

Version: 20130402:145459 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]