CORR 2000-04

Speeding up the Arithmetic on Koblitz Curves of Genus Two

Christian Günther*, Tanja Lange*, Andreas Stein

Abstract Koblitz, Solinas, and others investigated a family of elliptic curves which admit especially fast elliptic scalar multiplication. They considered elliptic curves defined over the finite field $\mathbb{F}_2$ with base field $\mathbb{F}_{2^n}$. In this paper, we generalize their ideas to hyperelliptic curves of genus 2. Given the two hyperelliptic curves $C_a : v^2 + uv = u^5 + a\,u^2 + 1$ with $a = 0, 1$, we show how to speed up the scalar multiplication in the Jacobian $\mathbb{J}_{C_a}(\mathbb{F}_{2^n})$ by making use of the Frobenius automorphism. With some precomputations, we are able to reduce the costs of the generic double-and-add-method in the Jacobian to approximately 19 percent. If we allow a few more precomputations, we are even able to reduce the costs to about 15 percent.