CORR 99-04

Computing Discrete Logarithms in High-Genus Hyperelliptic Jacobians in Provably Subexponential Time

Andreas Enge*

Abstract We provide a subexponential algorithm for solving the discrete logarithm problem in Jacobians of high-genus hyperelliptic curves over finite fields. More precisely, the running time for instances with genus g and underlying finite field $\mathbb{F}_q$ satisfying $g \geq \theta \log q$ for a positive constant θ is given by $O\left(e^{\left(\frac{5}{2\sqrt{3}}\left(\sqrt{1+\frac{3}{\theta}}+\sqrt{\frac{3}{\theta}}\right)+o(1)\right)\sqrt{(g\log q)\log(g\log q)}}\right)$. The algorithm works over any finite field, and its running time does not rely on any unproven assumptions.