

Cryptology ePrint Archive: Report 2013/095

A new index calculus algorithm with complexity $L(1/4+o(1))$ in very small characteristic

Antoine Joux

Abstract: In this paper, we describe a new algorithm for discrete logarithms in small characteristic. It works especially well when the characteristic is fixed. Indeed, in this case, we obtain a total complexity of $L(1/4+o(1))$.

Category / Keywords: foundations / Number Theory, Discrete Logarithms

Date: received 20 Feb 2013

Contact author: antoine joux at m4x org

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20130221:104921 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]