

Cryptology ePrint Archive: Report 2011/283

The Fault Attack ECDLP Revisited

Mingqiang Wang and Xiaoyun Wang and Tao Zhan

Abstract: Biehl et al. \cite{BMM} proposed a fault-based attack on elliptic curve cryptography. In this paper, we refined the fault attack method. An elliptic curve E is defined over prime field \mathbb{F}_p with base point $P \in E(\mathbb{F}_p)$. Applying the fault attack on these curves, the discrete logarithm on the curve can be computed in subexponential time of $L_p(1/2, 1+o(1))$. The runtime bound relies on heuristics conjecture about smooth numbers similar to the ones used in \cite{Lens}.

Category / Keywords: foundations /

Date: received 30 May 2011

Contact author: wangmingqiang at sdu edu cn

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

Version: 20110603:150026 ([All versions of this report](#))

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

[[Cryptology ePrint archive](#)]