Cryptology ePrint Archive: Report 2011/003

On the correct use of the negation map in the Pollard rho method

Daniel J. Bernstein and Tanja Lange and Peter Schwabe

Abstract: Bos, Kaihara, Kleinjung, Lenstra, and Montgomery recently showed that ECDLPs on the 112-bit secp112r1 curve can be solved in an expected time of 65 years on a PlayStation 3. This paper shows how to solve the same ECDLPs at almost twice the speed on the same hardware. The improvement comes primarily from a new variant of Pollard's rho method that fully exploits the negation map without branching, and secondarily from improved techniques for modular arithmetic.

Category / Keywords: public-key cryptography / Elliptic curves, discrete-logarithm problem, negation map, branchless algorithms, SIMD

Publication Info: Expanded version of PKC 2011 paper.

Date: received 1 Jan 2011

Contact author: tanja at hyperelliptic org