Cryptology ePrint Archive: Report 2011/461

Speeding Up Elliptic Curve Discrete Logarithm Computations with Point Halving

Fangguo Zhang and Ping Wang

Abstract: Pollard rho method and its parallelized variants are at present known as the best generic algorithms for computing elliptic curve discrete logarithms. We propose new iteration function for the rho method by exploiting the fact that point halving is more efficient than point addition for elliptic curves over binary fields. We present a careful analysis of the alternative rho method with new iteration function. Compared to the previous r-adding walk, generally the new method can achieve a significant speedup for computing elliptic curve discrete logarithms over binary fields. For instance, for certain NIST-recommended curves over binary fields, the new method is about 27\% faster than the previous best methods in single-instance Pollard rho method. When running several instances of Pollard rho method concurrently, and computing the inversions using the simultaneous inversion algorithm by Peter Montgomery, the new method is about 12-17\% faster than the previous best methods.

Category / Keywords:

Date: received 23 Aug 2011, last revised 29 Nov 2011

Contact author: isszhfg at mail sysu edu cn