Cryptology ePrint Archive: Report 2011/008

Computing Elliptic Curve Discrete Logarithms with the Negation Map

Ping Wang and Fangguo Zhang

Abstract: It is clear that the negation map can be used to speed up the computation of elliptic curve discrete logarithms with the Pollard rho method. However, the random walks defined on elliptic curve points equivalence class $\{\pm P\}$ used by Pollard rho will always get trapped in fruitless cycles. We propose an efficient alternative approach to resolve fruitless cycles. Besides the theoretical analysis, we also examine the performance of the new algorithm in experiments with elliptic curve groups. The experiment results show that we can achieve the speedup by a factor extremely close to $\sqrt{2}$, which is the best performance one can achieve in theory, using the new algorithm with the negation map.

Category / Keywords: public-key cryptography / elliptic curve cryptosystem

Date: received 5 Jan 2011

Contact author: isszhfg at mail sysu edu cn