Cryptology ePrint Archive: Report 2011/146

ECDLP on GPU

Lei Xu and Dongdai Lin and Jing Zou

Abstract: Elliptic curve discrete logarithm problem (ECDLP) is one of the most important hard problems that modern cryptography, especially public key cryptography, relies on. And many efforts are dedicate to solve this problem. In recent days, GPU technology develops very fast and GPU has become a powerful tool for massive computation. In this paper, we give an implementation of parallel Pollard method, for ECDLP on GPU, and eliminate nearly all the conditional branches in procedures for big integer, elliptic curve and iteration function. The experimental result shows that with the help of GPU, we can gain a speedup of more than one hundred times. The branchless procedures are also useful for preventing side channel attacks.

Category / Keywords: implementation / discrete logarithm problem, GPU

Date: received 23 Mar 2011, last revised 23 Mar 2011

Contact author: xuleimath at gmail com