World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:08, 2015

Solving 94-Bit ECDLP with 70 Computers in Parallel

Authors : Shunsuke Miyoshi, Yasuyuki Nogami, Takuya Kusaka, Nariyoshi Yamai

Abstract : Elliptic curve discrete logarithm problem (ECDLP) is one of problems on which the security of pairing-based cryptography is based. This paper considers Pollard's rho method to evaluate the security of ECDLP on Barreto-Naehrig (BN) curve that is an efficient pairing-friendly curve. Some techniques are proposed to make the rho method efficient. Especially, the group structure on BN curve, distinguished point method, and Montgomery trick are well-known techniques. This paper applies these techniques and shows its optimization. According to the experimental results for which a large-scale parallel system with MySQL is applied, 94-bit ECDLP was solved about 28 hours by parallelizing 71 computers.

Keywords : Pollard's rho method, BN curve, Montgomery multiplication
Conference Title : ICPBC 2015 : International Conference on Pairing-Based Cryptography
Conference Location : Paris, France
Conference Dates : August 27-28, 2015