World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:11, 2017

A Study of General Attacks on Elliptic Curve Discrete Logarithm Problem over Prime Field and Binary Field

Authors : Tun Myat Aung, Ni Ni Hla

Abstract : This paper begins by describing basic properties of finite field and elliptic curve cryptography over prime field and binary field. Then we discuss the discrete logarithm problem for elliptic curves and its properties. We study the general common attacks on elliptic curve discrete logarithm problem such as the Baby Step, Giant Step method, Pollard’s rho method and Pohlig-Hellman method, and describe in detail experiments of these attacks over prime field and binary field. The paper finishes by describing expected running time of the attacks and suggesting strong elliptic curves that are not susceptible to these attacks.c

Keywords : discrete logarithm problem, general attacks, elliptic curve, prime field, binary field
Conference Title : ICCIS 2017 : International Conference on Cryptography and Information Security
Conference Location : Bangkok, Thailand
Conference Dates : November 29-30, 2017