CORR 2000-42

Software Implementation of Elliptic Curve Cryptography Over Binary Fields

Darrel Hankerson*, Julio López Hernandez*, & Alfred Menezes

Abstract This paper presents an extensive and careful study of the software implementation on workstations of the NIST-recommended elliptic curves over binary fields. We also present the results of our implementation in C on the Pentium II 400 MHz workstation.