CORR 2000-56

Software Implementation of the NIST Elliptic Curves Over Prime Fields

M. Brown*, D. Hankerson*, J. López*, and A. Menezes

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