

5th Workshop on Elliptic Curve Cryptography (ECC 2001), University of Waterloo, Canada, October 29-31, 2001.

Speaker

Darrel Hankerson

Title

Performance comparisons of elliptic curve systems in software

Abstract

Implementing elliptic curve cryptographic schemes involves many design decisions including underlying field (prime, Mersenne-like prime, characteristic two, optimal extension), curve (randomly selected, Koblitz, Gallant), memory usage, and implementation language (C or assembler).

We present and compare the results of our software implementation of these various flavours of elliptic (and hyperelliptic) curve systems.

<http://www.cacr.math.uwaterloo.ca/>