CORR 99-33

The Elliptic Curve Digital Signature Algorithm (ECDSA)

Don Johnson* & Alfred Menezes

Abstract The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA), and was accepted in 1999 as an ANSI standard. It is also under consideration for standardization by IEEE P1363, ISO SC27, and NIST. Unlike the ordinary discrete logarithm problem and the integer factorization problem, no subexponential-time algorithm is known for the elliptic curve discrete logarithm problem. For this reason, the strength-per-key-bit is substantially greater in an algorithm that uses elliptic curves. This paper describes the ANSI X9.62 ECDSA, and discusses related security, implementation, and interoperability issues.

Keywords Signature schemes, elliptic curve cryptography, DSA, ECDSA.