{tag} {/tag} International Journal of Computer Applications

Number 2 - Article 5

Year of Publication: 2010

Authors:

Aqeel Khalique

Kuldip Singh

Sandeep Sood

10.5120/631-876

{bibtex}pxc387876.bib{/bibtex}

Abstract

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). It was accepted in 1999 as an ANSI standard, and was accepted in 2000 as IEEE and NIST standards. It was also accepted in 1998 as an ISO standard, and is under consideration for inclusion in some other ISO standards. Unlike the ordinary discrete logarithm problem and the integer factorization problem, no sub exponential-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 implementation of ANSI X9.62 ECDSA over elliptic curve P-192, and discusses related security issues.

Reference

- Vanstone, S. A., 1992. Responses to NIST's Proposal Communications of the ACM, 35, 50-52.
- Vanstone, S. A., 2003. Next generation security for wireless: elliptic curve cryptography.

Computers and Security, vol. 22, No. 5.

- Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of Computation 48, 203-209.
- Miller, V., 1985. Use of elliptic curves in cryptography. CRYPTO 85.
- Certicom ECC Challenge. 2009. Certicom Research
- Hankerson, D., Menezes, A., Vanstone, S., 2004. Guide to Elliptic Curve Cryptography. Springer.
- Botes, J.J., Penzhorn, W.T., 1994. An implementation of an elliptic curve cryptosystem. Communications and Signal Processing. COMSIG-94. In Proceedings of the 1994 IEEE South African Symposium, 85 -90.
- An intro to Elliptical Curve Cryptography[On-Line]. Available:http://www.deviceforge.com/articles/AT4234154468.html [2010].
- Gupta, V., Stebila, D., Fung, S., Shantz, S.C., Gura, N., Eberle, H., 2004. Speeding up Secure Web Transactions Using Elliptic Curve Cryptography. In Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS 2004). The Internet Society, 231-239.
- Raju, G.V.S., Akbani, R., 2003. Elliptic Curve Cryptosystem And Its Application. In Proceedings of the 2003 IEEE International Conference on Systems Man and Cybernetics (IEEE-SMC), 1540-1543.
- Johnson, D.B., Menezes, A.J., 2007. Elliptic Curve DSA (ECDSA): An Enhanced DSA. Scientific Commons.

Index Terms

Computer Science Security

Key words

Integer factorization

Discrete logarithm problem

Elliptic curve cryptography

DSA

ECDSA