{tag}

{/tag}

International Journal of Computer Applications

Number 1 - Article 1

Year of Publication: 2011

Authors:

W. R. Sam Emmanuel

C. Suyambulingom

10.5120/3944-5582

{bibtex}pxc3875582.bib{/bibtex}

Abstract

This paper proposes Probability Symmetric Curve Cryptography (PSCC), which is a new milestone in the Symmetric Curve Cryptography. The PSCC proposes the new approach to do the point addition and point doubling. The finite field operations applied in the PSCC provides the new spirit of thinking more on the safety of the data. This paper also expresses the usage

of domain parameters and key pair creation. The results of this approach express the security of data in terms of future technology. The overall objective is to generate valuable dynamic security measures using PSCC.

Reference

- William Stallings, “Cryptography and Network Security Principles and Practices”, 3rd Ed., Pearson Education, 2004.
- Lee L. P. and Wong K. W., “A random number generator based elliptic curve operations”, Computers and Mathematics with Applications, vol. 47, pp. 217-226, 2004.
- Nel Koblitz, Algred Menezes and Scott Vanstone, “The state of elliptic curve cryptography, Journal of Designs”, Codes and Cryptography, vol.19, pp.173-193, 2000.
- Menezes A., “Elliptic Curve Public Key Cryptosystems”, Kluwer Academic Publishers, 1993.
- Atay S., Kottuksuz A, Hisil H. and Eren S., “Computational cost analysis of elliptic curve arithmetic”, Proceedings of international conference on Hybrid Information Technology (ICHIT ’06), vol.1, pp.578-582, 2006.
- Vivek Kapoor, Vivek Sonny Abraham and Ramesh Singh, “Elliptic Curve Cryptography”, ACM Ubiquity, vol.9, pp.1-8, 2008.
- Alfred J Menezes and Scott A Vanstone, “Elliptic curve cryptosystems and their implementation”, Journal of Cryptology, vol.6(4), pp.209-224, 2004.
- Gong G., Berson T. A. and Stinson D. R., “Elliptic curve pseudorandom sequence generators”, Proceedings of the 6th Annual International Workshop on Selected Areas in Cryptography, LNCS 1758, pp 34-48, 1999.
- Shi Z. J. and Yan H., “Software implementations of elliptic curve cryptography”, International Journal of Network Security, vol. 7(1), pp. 141-150, 2008.
- Berkhoff G. and Lane S. M., “A Survey of Modern Algebra”, AKP Classics, USA, 2008.
- Koblitz N., “A Course in Number Theory and Cryptography”, Springer Verlag, New York, 1984.
- Jarvinen K, Tommiska M. and Skytta J., “A scalable architecture for elliptic curve point multiplication”, Proceedings of IEEE international conference on Field-Programmable Technology, pp.303-306, 2004.
- ElGamal T., “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information theory, vol. IT-31, pp.469-472, 1985.
- Hansen T. and Mullen G. L., “Primitive polynomials over finite fields”, Mathematics of Computation, vol.59(200), pp. 639-643, 1992.
- Morain F., “Building cyclic elliptic curves modulo large primes”, LNCS 547, pp. 328-336, 1990.
- http://en.wikipedia.org/wiki/List_of_curves.
- Sam Emmanuel W.R. and Suyambulingom C., “Safety Measures Using Sextic Curve Cryptography”, International Journal on Computer Science and Engineering, vol.3(2), pp.800-806,2011.

Index Terms

Computer Science Security

Key words

Probability Symmetric Curve Cryptography Point Addition
Point Doubling
Domain
Parameters