MATHEMATICA, Tome 50 (73), N° 2, 2008, pp. 177–186

NON SINGULAR ELLIPTIC CURVES–FROM THEORY TO APPLICATION. ALGORITHM ATTACKS DISCUSSIONS

NICOLAE CONSTANTINESCU

Abstract. Let E be an elliptic curve. Starting from its definition we create a set of restrictions which helps us to realize an implementation in a real system of the theories concerning the infeasibility of the ECDL problem. We also present the implementation methods to compute the necessary parameters in such a system.

MSC 2000. 11G07.
Key words. Elliptic curves, public key cryptography.

REFERENCES

[1] Blake, I. F., Seroussi, G. and Smart, N. P., *Elliptic Curves in Cryptography*, Cambridge University Press, 2002.
[2] Crandall, R., *Method and apparatus for public key exchange in a cryptographic system*, U. S. Patent Number 5159632.
[3] Lercier, R. and Morain, F., *Counting points in elliptic curves over F_{p^n} using Couveignes algorithm*, Rapport de Recherche LIX/RR/95/09.1995.
[4] Lercier, R., *Computing isogenies in F_{2^n}*, White Paper, 197–212.
[5] van Lint, J. T., *Introduction to Coding Theory*, Springer-Verlag, 1982.
[6] Montgomery, P. L., *Modular multiplication without trial division*, Math. Comp., **44**, 519–521, 1985.
[7] Pohlig, G. L. and Hellman, M. E., *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic signifiance*, IEEE Trans. Info. Theory, **24**, 1978, 106–110.
[8] Smart, N. P., *Elliptic curves over small fields of odd characteristic*, Journal of Cryptography, **12**, 141–151, 1999.
[9] Solinas, J. A., *An improved algorithm for arithmetic on a family of elliptic curves*, Springer-Verlag, 1997.
[10] Stinson, D. R., *Cryptography - Theory and Practice*, CRC Press, 2002.
[11] Certicom White Paper, *The elliptic curve cryptosystem for smart card*, Published: May 1998.
[12] Agnew, G., Mullin, R. and Vanstone, S., *An implementation of elliptic curve cryptosystem over $F_{2^{155}}$*, IEEE Journal on Selected Areas in Communications, **11** (1993), 804–813.
[13] Gao, S., von Zur Gathen, J., Panario, D. and Shoup, V., *Algorithms for Exponentiation in Finite Fields*, Journal of Symbolic Computation 2000, **29**, 879–889.
[14] Lim, C. and Lee, P., *A key recovery attack on discrete log-based schemes using a prime order subgroup*, Advances in Cryptography 1997, **1294** (1997), Springer-Verlag, Lecture Notes in Computer Science, 275–288.
[15] van Oorschot, P. C. and Wiener, M. J., *Parallel Collision Search with Cryptanalytic Applications*, Journal of Cryptology, **12** (1999) , Springer - Verlag, 1–28.

Received August 06, 2007

University of Craiova,
Computer-Science Department
A.I. Cuza street, no. 13, Craiova, Romania
E-mail: nikyc@central.ucv.ro