Gustavsen, Trond Stølen; **Ranestad, Kristian**

A simple point counting algorithm for Hessian elliptic curves in characteristic three. (English) Zbl 1099.14011

Appl. Algebra Eng. Commun. Comput. 17, No. 2, 141-150 (2006).

Summary: Given an ordinary elliptic curve on Hesse form over a finite field of characteristic three, we give a sequence of elliptic curves which leads to an effective construction of the canonical lift, and obtain an algorithm for computing the number of points. Our methods are based on the study of an explicitly and naturally given 3-isogeny between elliptic curves on Hesse form.

MSC:

14G50 Applications to coding theory and cryptography of arithmetic geometry
94A60 Cryptography

Cited in **2** Documents

Keywords:

finite field; point counting; cryptography

Software:

PARI/GP

Full Text: DOI

References:

[1] Carls, R.: A generalized arithmetic geometric mean. PhD Thesis (2004). http://www.maths.usyd.edu.au/u/carls/thesis.pdf

[2] Deuring M. (1941). Die Typen der Multiplikatorringe Elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg 14:197–272 · Zbl 0025.02003 · doi:10.1007/BF02940746

[3] Frium H.R. The group law on elliptic curves on Hesse form. In: Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), pp. 123–151. Berlin Heidelberg New York: Springer 2002 · Zbl 1057.14038

[4] Harrison K., Page D., Smart N.P. (2002). Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems. LMS J Comput Math 5:181–193 (electronic) · Zbl 1068.94012

[5] Joye, M., Quisquater, J.J.: Hessian elliptic curves and side-channel attacks. In: Cryptographic hardware and embedded systems – CHES 2001 (Paris), Lecture Notes in Comput Sci, vol. 2162, pp. 402–410. Berlin Heidelberg New York: Springer 2001 · Zbl 1012.94547

[6] Kohel, D.R.: The AGM-X 0(N) Heegner point lifting algorithm and elliptic curve point counting. In: Advances in cryptology – ASIACRYPT 2003 (Taipei, Taiwan), Lecture Notes in Comput Sci, vol. 2894, pp. 124–136. Berlin Heidelberg New York: Springer 2003 · Zbl 1205.11071

[7] Lang S. (1987). Elliptic Functions, 2nd edn. Springer, Berlin Heildelberg New York · Zbl 0615.14018

[8] Madsen, M.S.: The AGM-method of point counting on ordinary elliptic curves over finite fields of characteristic 2. (2002). http://home.imf.au.dk/marc

[9] Mestre, J.F.: Lettre adressée à Gaudry et Harley. http://www.math.jussieu.fr/mestre (2000)

[10] Page D., Smart N.P. (2003). Hardware implementation of finite fields of characteristic three. In: Kaliski B.S Jr., Koç C.K., Paar C. (eds) Cryptographic hardware and embedded systems – CHES 2002. Springer, Berlin Heidelberg New York, pp. 529–539 · Zbl 1028.68003

[11] Satoh T. (2000). The canonical lift of an ordinary elliptic curve over a finite field and its point counting. J Ramanujan Math Soc 115(4):247–270 · Zbl 1009.11051

[12] Satoh T., Skjernaa B., Taguchi Y. (2003). Fast computation of canonical lifts of elliptic curves and its application to point counting. Finite Fields Appl 9:89–101 · Zbl 1106.14302 · doi:10.1016/S1071-5797(02)00013-8

[13] Schoof R. (1985). Elliptic curves over finite fields and the computation of square roots mod p. Math. Comp. 44(170): 483–494 · Zbl 0579.14025

[14] Smart N.P. (2001). The Hessian form of an elliptic curve. In: C.P. C.K. Koc D. Naccache (ed.) Cryptographic hardware and embedded systems CHES 2001, no. 2162 in Lecture Notes in Comput. Sci., pp. 118–126. Berlin Heidelberg New York: Springer · Zbl 1021.94522

[15] Smart N.P., Westwood E.J. (2003). Point multiplication on ordinary elliptic curves over fields of characteristic three. Appl Algebra Eng Comm Comput 13(6):485–497 · Zbl 1034.94008 · doi:10.1007/s00200-002-0114-0

[16] The PARI Group, Bordeaux: PARI/GP, Version 2.1.5 (2000). http://www.parigp-home.de/

[17] Vercauteren, F., Preneel, B., Vandewalle, J.: A memory efficient version of Satoh's algorithm. In: Advances in cryptology – EUROCRYPT 2001 (Innsbruck), Lecture Notes in Comput Sci, vol. 2045, pp. 1–13. Berlin Heidelberg New York: Springer 2001 · Zbl 1009.11052