Satoh, Takakazu; **Skjernaa, Berit**; **Taguchi, Yuichiro**

Fast computation of canonical lifts of elliptic curves and its application to point counting.

(English) Zbl 1106.14302
Finite Fields Appl. 9, No. 1, 89-101 (2003).

Summary: Let p be a fixed small prime. We give an algorithm with preprocessing to compute the j-invariant of the canonical lift of a given ordinary elliptic curve $E/\mathbb{F}_q$ ($q = p^N$, $j(E) \notin F_{p^2}$) modulo $p^{N/2+O(1)}$ in $O(N^{2\mu+1/\mu+1})$ bit operations (assuming the time complexity of multiplying two n-bit objects is $O(n^\mu)$) using $O(N^2)$ memory, not including preprocessing. This is faster than the algorithm of *F. Vercauteren* et al. [Lect. Notes Comput. Sci. 2045, 1–13 (2001; Zbl 1009.11052)] by a factor of $N^{\mu/\mu+1}$. Let K be the unramified extension field of degree N over $\mathbb{Q}_p$. We also develop an algorithm to compute $N_{K/\mathbb{Q}_p}(x) \pmod p^{N/2+O(1)}$ with $O(N^{2\mu+0.5})$ bit operations and $O(N^2)$ memory when $x \in K$ satisfies certain conditions, which are always satisfied when applied to our point counting algorithm. As a result, we get an $O(N^{2\mu+0.5})$ time, $O(N^2)$ memory algorithm for counting the $\mathbb{F}_q$-rational points on $E/\mathbb{F}_q$, which turns out to be very fast in practice for cryptographic size elliptic curves.

MSC:

14G50	Applications to coding theory and cryptography of arithmetic geometry
11Y16	Number-theoretic algorithms; complexity
11G20	Curves over finite and local fields
14G05	Rational points

Keywords:

elliptic curves; canonical lifts; Frobenius substitutions

Full Text: DOI

References:

[1] Aho, A.V.; Hopcroft, J.E.; Ullman, J.D., The design and analysis of computer algorithms, (1974), Addison-Wesley Reading, MA · Zbl 0326.68005

[2] N.D. Elkies, Elliptic and modular curves over finite fields and related computational issues, Computational Perspectives on Number Theory, Chicago, IL, 1995; AMS/IP Studies in Advanced Mathematics, Vol. 7, AMS, Providence, RI, 1998, pp. 21-76. · Zbl 0915.11036

[3] Fouquet, M.; Gaudry, P.; Harley, R., An extension of Satoh's algorithm and its implementation, J. Ramanujan math. soc., 15, 281-318, (2000) · Zbl 1009.11048

[4] Fröhlich, A.; Taylor, M.J., Algebraic number theory, Cambridge studies in advanced mathematics, Vol. 27, (1993), Cambridge Univ. Press Cambridge · Zbl 0744.11001

[5] R. Harley, Counting points with the arithmetic – geometric mean (joint work with J.-F. Mestre and P. Gaudry), Eurocrypt 2001, Rump session, 2001.

[6] Kedlaya, K., Counting points on hyperelliptic curves using monsky – washnitzer cohomology, J. Ramanujan math. soc., 16, 323-338, (2001) · Zbl 1066.14024

[7] Koblitz, N., Elliptic curve cryptosystems, Math. comput., 48, 203-209, (1987) · Zbl 0622.94015

[8] J. Lubin, J.-P. Serre, J. Tate, Elliptic curves and formal groups, Mimeographed Notes, 1964, available at http://www.ma.utexas.edu/users/voloch/ls

[9] V.S. Miller, Use of elliptic curves in cryptography, Advances in Cryptology—CRYPTO '85, Santa Barbara, CA, 1985, Lecture Notes in Computer Science, Vol. 218, Springer, Berlin, Heidelberg, New York, 1986, pp. 417-426.

[10] Satoh, T., The canonical lift of an ordinary elliptic curve over a finite field and its point counting, J. Ramanujan math. soc., 15, 247-270, (2000) · Zbl 1009.11051

[11] T. Satoh, On \textit{p}-adic point counting algorithms for elliptic curves over finite fields, In: C. Fieker, D. Kohel (Eds.), Algorithmic number theory, Proceeding of ANTS-5, 2002 (Sydney, Australia, July 2002), Lecture Notes in Computer Science, Vol. 2369, Springer, Berlin, 2002, pp. 43-66. · Zbl 1058.11043

[12] Schoof, R., Elliptic curves over finite fields and the computation of square roots mod \textit{p}, Math. comput., 44, 483-494, (1985) · Zbl 0579.14025

[13] Skjernaa, B., Satoh's algorithm in characteristic 2, Math. comput., 72, 447-487, (2003) · Zbl 1027.11045

[14] F. Vercauteren, B. Preneel, J. Vandewalle, A memory efficient version of Satoh's algorithm, in: B. Pfitzmann (Ed.), Advances in Cryptology—Eurocrypt 2001, Innsbruck, Austria, May 2001, Lecture Notes in Computer Science, Vol. 2045, Springer, Berlin, Heidelberg, 2001, pp. 1-13. · Zbl 1009.11052