Joux, Antoine; **Lercier, Reynald**

Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the Gaussian integer method. (English) Zbl 1099.11074

Math. Comput. 72, No. 242, 953-967 (2003).

Summary: We describe many improvements to the number field sieve. Our main contribution consists of a new way to compute individual logarithms with the number field sieve without solving a very large linear system for each logarithm. We show that, with these improvements, the number field sieve outperforms the gaussian integer method in the hundred digit range. We also illustrate our results by successfully computing discrete logarithms with GNFS in a large prime field.

MSC:

11Y16 Number-theoretic algorithms; complexity
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
11Y40 Algebraic number theory computations
68Q25 Analysis of algorithms and problem complexity
94A60 Cryptography

Full Text: DOI

References:

[1] L.M. Adleman, Factoring numbers using singular integers, Proceedings 23rd Annual ACM Symposium on Theory of Computing (STOC), 1991, pp. 64-71.

[2] Derek Atkins, Michael Graff, Arjen K. Lenstra, and Paul C. Leyland, The magic words are squeamish ossifrage (extended abstract), Advances in cryptology — ASIACRYPT '94 (Wollongong, 1994) Lecture Notes in Comput. Sci., vol. 917, Springer, Berlin, 1995, pp. 263 – 277. · Zbl 0877.94026

[3] D. J. Bernstein and A.K. Lenstra, A general number field sieve implementation, Springer-Verlag, 1993, pp. 103-126. CMP 95:09 · Zbl 0806.11069

[4] J. Buchmann, J. Loho, and J. Zayer, An implementation of the general number field sieve (extended abstract), Advances in cryptology — CRYPTO '93 (Santa Barbara, CA, 1993) Lecture Notes in Comput. Sci., vol. 773, Springer, Berlin, 1994, pp. 159 – 165. · Zbl 0871.11092 · doi:10.1007/3-540-48329-2_14 · doi.org

[5] J.P. Buhler, Jr. H.W. Lenstra, and Carl Pomerance, Factoring integer with the number field sieve, Springer-Verlag, 1993, pp. 50-94 (see [26]). CMP 95:09 · Zbl 0806.11067

[6] Stefania Cavallar, Strategies in filtering in the number field sieve, Algorithmic number theory (Leiden, 2000) Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 209 – 231. · Zbl 1006.11076 · doi:10.1007/10722028_11 · doi.org

[7] S. Cavallar, B. Dodson, A.K. Lenstra, W. Lioen, , P.L. Montgomery, B. Murphy, H. te Riele, K. Aardal, J. Gilchrist, G. Guillerm, P. Leyland, J. Marchand, F. Morain, A. Muffet, C. Putman, C. Putman, and P. Zimmerman, Factorization of a 512-bit RSA modulus, Advances in Cryptology – EUROCRYPT'2000 , Lecture Notes in Computer Science, vol. 1807, Springer-Verlag, 2000, pp. 1-18. · Zbl 1082.94511

[8] Stefania Cavallar, Bruce Dodson, Arjen Lenstra, Paul Leyland, Walter Lioen, Peter Mongomery, Brian Murphy, Herman te Riele, and Paul Zimmerman, Factorization of RSA-140, http://listserv.nodak.edu/archives/nmbrthry.html – February, 1999. · Zbl 0971.94008

[9] Don Coppersmith, Fast evaluation of logarithms in fields of characteristic two, IEEE Trans. Inform. Theory 30 (1984), no. 4, 587 – 594. · Zbl 0554.12013 · doi:10.1109/TIT.1984.1056941 · doi.org

[10] Don Coppersmith, Andrew M. Odlzyko, and Richard Schroeppel, Discrete logarithms in \?\?(\?), Algorithmica 1 (1986), no. 1, 1 – 15. · Zbl 0631.12010 · doi:10.1007/BF01840433 · doi.org

[11] J.-M. Couveignes, Computing a square root for the number field sieve, Springer-Verlag, 1993, pp. 95-102 (see [26]). CMP 95:09

[12] J. Cowie, B. Dodson, R. M. Elkenbracht-Huizing, A. K. Lenstra, P. L. Montgomery, and J. Zayer, A world wide number field sieve factoring record: On to 512 bits, Advances in Cryptology – ASIACRYPT'96 , Lecture Notes in Computer Science, vol. 1163, Springer-Verlag, 1996, pp. 382-394. CMP 98:05 · Zbl 1028.11500

[13] Thomas F. Denny and Volker Müller, On the reduction of composed relations from the number field sieve, Algorithmic number theory (Talence, 1996) Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 75 – 90. · Zbl 0943.11056 · doi:10.1007/3-540-61581-4_43 · doi.org

[14] Bruce Dodson and Arjen K. Lenstra, NFS with four large primes: an explosive experiment, Advances in cryptology —

CRYPTO '95 (Santa Barbara, CA, 1995) Lecture Notes in Comput. Sci., vol. 963, Springer, Berlin, 1995, pp. 372 – 385. · Zbl 0883.11054 · doi:10.1007/3-540-44750-4_30 · doi.org

[15] R.-M. Elkenbracht-Huizing, Peter L. Montgomery, R. D. Silverman, R. K. Wackerbarth, and S. S. Wagstaff Jr., The number field sieve on many computers, Number theory (Ottawa, ON, 1996) CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, pp. 81 – 85. · Zbl 0936.11070

[16] Marije Elkenbracht-Huizing, An implementation of the number field sieve, Experiment. Math. 5 (1996), no. 3, 231 – 253. · Zbl 0869.11101

[17] Marije Elkenbracht-Huizing, A multiple polynomial general number field sieve, Algorithmic number theory (Talence, 1996) Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 99 – 114. · Zbl 0899.11060 · doi:10.1007/3-540-61581-4_45 · doi.org

[18] Roger A. Golliver, Arjen K. Lenstra, and Kevin S. McCurley, Lattice sieving and trial division, Algorithmic number theory (Ithaca, NY, 1994) Lecture Notes in Comput. Sci., vol. 877, Springer, Berlin, 1994, pp. 18 – 27. · Zbl 0838.11080 · doi:10.1007/3-540-58691-1_38 · doi.org

[19] Daniel M. Gordon, Discrete logarithms in \?\?(\?) using the number field sieve, SIAM J. Discrete Math. 6 (1993), no. 1, 124 – 138. · Zbl 0772.11046 · doi:10.1137/0406010 · doi.org

[20] D. Gordon and K. McCurley, Massively parallel computation of discrete logarithms, Advances in Cryptology – CRYPTO'92, Lecture Notes in Computer Science, vol. 740, Springer-Verlag, 1993, pp. 312-323. · Zbl 0813.94007

[21] A. Joux, La réduction de réseaux en cryptographie, Ph.D. thesis, Ecole Polytechnique, Palaiseau, France, 1993.

[22] Antoine Joux and Jacques Stern, Lattice reduction: a toolbox for the cryptanalyst, J. Cryptology 11 (1998), no. 3, 161 – 185. · Zbl 0919.94011 · doi:10.1007/s001459900042 · doi.org

[23] Antoine Joux and Reynald Lercier, Discrete logarithms in GF(p), http://listserv.nodak.edu/archives/nmbrthry.html – May, 1998. · Zbl 1235.11116

[24] B. A. LaMacchia and A. M. Odlyzko, Computation of discrete logarithms in prime fields, Des. Codes Cryptogr. 1 (1991), no. 1, 47 – 62. · Zbl 0747.94012 · doi:10.1007/BF00123958 · doi.org

[25] -, Solving large sparse linear systems over finite fields, Advances in Cryptology – CRYPTO'90, Lecture Notes in Computer Science, vol. 537, Springer-Verlag, 1991, pp. 109-133. · Zbl 0786.65028

[26] A. K. Lenstra and H. W. Lenstra Jr. , The development of the number field sieve, Lecture Notes in Mathematics, vol. 1554, Springer-Verlag, Berlin, 1993. · Zbl 0777.00017

[27] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, Factoring polynomials with rational coefficients, Math. Ann. 261 (1982), no. 4, 515 – 534. · Zbl 0488.12001 · doi:10.1007/BF01457454 · doi.org

[28] A. K. Lenstra, H. W. Lenstra Jr., M. S. Manasse, and J. M. Pollard, The factorization of the ninth Fermat number, Math. Comp. 61 (1993), no. 203, 319 – 349. · Zbl 0792.11055 ·

[29] -, The number field sieve, Springer-Verlag, 1993, pp. 11-42 (see [26]). CMP 95:09

[30] Kevin S. McCurley, The discrete logarithm problem, Cryptology and computational number theory (Boulder, CO, 1989) Proc. Sympos. Appl. Math., vol. 42, Amer. Math. Soc., Providence, RI, 1990, pp. 49 – 74. · doi:10.1090/psapm/042/1095551 · doi.org

[31] Peter L. Montgomery, A block Lanczos algorithm for finding dependencies over \?\?(2), Advances in cryptology — EUROCRYPT '95 (Saint-Malo, 1995) Lecture Notes in Comput. Sci., vol. 921, Springer, Berlin, 1995, pp. 106 – 120. · Zbl 0973.11520 · doi:10.1007/3-540-49264-X_9 · doi.org

[32] A. M. Odlyzko, Discrete logarithms in finite fields and their cryptographic significance, Advances in cryptology (Paris, 1984) Lecture Notes in Comput. Sci., vol. 209, Springer, Berlin, 1985, pp. 224 – 314. · Zbl 0594.94016 · doi:10.1007/3-540-39757-4_20 · doi.org

[33] J.M. Pollard, Factoring with cubic integer, Springer-Verlag, 1993, pp. 4-10 (see [26]). CMP 95:09

[34] -, The lattice sieve, Springer-Verlag, 1993, pp. 43-49. CMP 95:09

[35] Oliver Schirokauer, Discrete logarithms and local units, Philos. Trans. Roy. Soc. London Ser. A 345 (1993), no. 1676, 409 – 423. · Zbl 0795.11063 · doi:10.1098/rsta.1993.0139 · doi.org

[36] Oliver Schirokauer, Damian Weber, and Thomas Denny, Discrete logarithms: the effectiveness of the index calculus method, Algorithmic number theory (Talence, 1996) Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 337 – 361. · Zbl 0895.11054 · doi:10.1007/3-540-61581-4_66 · doi.org

[37] RSA Data Security, The RSA factoring challenge, http://www.rsa.com/rsalabs/html/factoring.html.

[38] Robert D. Silverman, The multiple polynomial quadratic sieve, Math. Comp. 48 (1987), no. 177, 329 – 339. · Zbl 0608.10004 ·

[39] F. Valette, Algèbre linéaire pour le logarithme discret, Master's thesis, ENSTA, 1999, Stage de fin d'étude et de DEA.

[40] Damian Weber, Computing discrete logarithms with the general number field sieve, Algorithmic number theory (Talence, 1996) Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 391 – 403. · Zbl 0899.11061 · doi:10.1007/3-540-61581-4_70 · doi.org

[41] -, Computing discrete logarithms with quadratic number rings, Advances in Cryptology – EUROCRYP'98 , Lecture Notes in Computer Science, vol. 1403, Springer-Verlag, 1998, pp. 171-183. CMP 2000:07

[42] Damian Weber and Thomas Denny, The solution of McCurley's discrete log challenge, Advances in cryptology — CRYPTO '98 (Santa Barbara, CA, 1998) Lecture Notes in Comput. Sci., vol. 1462, Springer, Berlin, 1998, pp. 458 – 471. · Zbl 0945.11026 · doi:10.1007/BFb0055747 · doi.org