# References


[1] Daniel J. Bernstein. Bounding smooth integers. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 128–130. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[2] Antonia W. Bluher. Formal groups, elliptic curves, and some theorems of couveignes. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 482–501. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[3] Dan Boneh. The decision diffie-hellman problem. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 48–63. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[4] Dan Boneh and Jeremy Horwitz. Generating a product of three primes with an unknown factorization. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 237–251. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[5] Giovanni Cesari. Parallel implementation of schönhage's integer gcd algorithm. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 64–76. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[6] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Computation of relative quadratic class groups. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory,*

*ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 433–440. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[7] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Imprimitive octic fields with small discriminants. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 372–380. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[8] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. A table of totally complex number fields of small discriminats. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 381–391. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[9] Bart de Smit. Generating arithmetically equivalent number fields with elliptic curves. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 392–399. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[10] Erik de Win, Serge Mister, Bart Preneel, and Michael Wiener. On the performance of signature schemes based on elliptic curves. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 252–266. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[11] J.-M. Deshouillers, H.J.J. te Riele, and Y. Saouter. New experimental results concerning the goldbach conjecture. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423

of *LNCS*, pages 204–215. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[12] Jean-Marc Deshouillers, François Hennecart, and Bernard Landreau. Do sums of 4 biquadrates have a positive density? In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 196–203. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[13] Z. Djabri and N.P. Smart. A comparison of direct and indirect methods for computing selmer groups of an elliptic curve. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 502–513. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[14] David S. Dummit and Brett A. Tangedal. Computing the lead term of an abelian $l$-function. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 400–411. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[15] Noam D. Elkies. Shimura curve computations. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 1–47. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[16] William F. Galway. Robert bennion's "hopping sieve". In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 169–178. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[17] Alice Gee and Peter Stevenhagen. Generating class fields using shimura reciprocity. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 441–453. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[18] Daniel M. Gordon and Gene Rodemich. Dense admissible sets. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 216–225. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[19] Bruno Haible and Thomas Papanikolaou. Fast multiprecision evaluation of series of rational numbers. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 338–350. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[20] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Ntru: A ring-based public key cryptosystem. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 267–288. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[21] Joshua Holden. Irregularity of prime numbers over real quadratic fields. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 454–462. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[22] Ming-Deh Huang and Yiu-Chung Wong. An algorithm for approximate counting of points on algebraic sets over finite fields. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25,*

*1998)*, volume 1423 of *LNCS*, pages 514–527. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[23] Jr. Jacobson, Michael J. Experimental results on class groups of real quadratic fields. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 463–474. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[24] John W. Jones and David P. Roberts. Timing analysis of targeted hunter searches. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 412–423. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[25] Stéphane Louboutin. Computation of relative class numbers of imaginary cyclic fields of 2-power degrees. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 475–481. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[26] Jacques Martinet. On successive minima of rings of algebraic integers. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 424–432. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[27] Preda Mihăilescu. Cyclotomy primality proving — recent developments. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 95–110. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[28] F. Morain. Primality proving using elliptic curves: An update. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 111–127. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[29] Brian Murphy. Modelling the yield of number field sieve polynomials. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 137–150. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[30] Stefan Neis. Reducing ideal arithmetic to linear algebra problems. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 299–310. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[31] Phong Nguyen. A montgomery-like square root for the number field sieve. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 151–168. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[32] Harald Niederreiter and Chaoping Xing. A general method of constructing global function fields with many rational places. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 555–566. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[33] Daniel Panario, Xavier Gourdon, and Philippe Flajolet. An analytic approach to smooth polynomials over finite fields. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25,*

*1998)*, volume 1423 of *LNCS*, pages 226–236. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[34] Sachar Paulus. Lattice basis reduction in function fields. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 567–575. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[35] Sachar Paulus and Andreas Stein. Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 576–591. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[36] A. Pethő, E. Herrmann, and H.G. Zimmer. $s$-integral points on elliptic curves and fermat's triple equations. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 528–540. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[37] Renate Scheidler and Andreas Stein. Unit computation in purely cubic function fields of unit rank 1. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 592–606. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[38] I.A. Semaev. Evaluation of linear relations between vectors of a lattice in euclidean space. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 311–322. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[39] Jonathan P. Sorenson. Trading time for space in prime number sieves. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 179–195. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[40] Andreas Stein and Hugh C. Williams. An improved method of computing the regulator of a real quadratic function field. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 607–620. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[41] E. Teske and H.C. Williams. A problem concerning a character sum. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 351–357. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[42] Edlyn Teske. Speeding up pollard's rho method for computing discrete logarithms. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 541–554. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[43] Brigitte Vallée. The complete analysis of the binary euclidean algorithm. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 77–94. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[44] Alf van der Poorten. Formal power series and their continued fraction expansion. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Port-*

*land, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 358–371. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[45] Susanne Wetzel. An efficient parallel block-reduction algorithm. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 323–337. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[46] Adam Young and Moti Yung. Finding length-3 positive cunningham chains and their cryptographic significance. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 289–298. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[47] Mingzhi Zhang. Factorization of the numbers of the form $m^3 + c_2m^2 + c_1m+c_0$. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 131–136. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.

[48] Robert J. Zuccherato. The equivalence between elliptic curve and quadratic function field discrete logarithms in characteristic 2. In J.P. Buhler, editor, *Proceedings of the 3rd International Symposium on Algorithmmic Number Theory, ANTS'98 (Portland, Oregon, June 21-25, 1998)*, volume 1423 of *LNCS*, pages 621–638. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Budapest-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1998.