References

[1] Seigo Arita. Construction of secure c_{ab} curves using modular curves. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 113–126. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[2] Roland Auer. Curves over finite fields with many rational points obtained by ray class field extensions. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 127–134. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[3] Werner Backes and Susanne Wetzel. New results on lattice basis reduction in practice. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 135–152. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[4] Simon R. Blackburn and Edlyn Teske. Baby-step giant-step algorithms for non-uniform distributions. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 153–168. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[5] Nils Bruin. On powers as sums of two cubes. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 169–184. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[6] Jin-Yi Cai. The complexity of some lattice problems. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*,

volume 1838 of *LNCS*, pages 1–32. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[7] David G. Cantor and Daniel M. Gordon. Factoring polynomials over p-adic fields. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 185–208. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[8] Stefania Cavallar. Strategies in filtering in the number field sieve. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 209–231. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[9] Qi Cheng and Ming-Deh A. Huang. Factoring polynomials over finite fields and stable colorings of tournaments. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 233–245. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[10] Gautam Chinta, Paul E. Gunnells, and Robert Sczech. Computing special values of partial zeta functions. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 247–256. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[11] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Construction of tables of quartic number fields. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 257–268. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[12] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Counting discriminants of number fields of degree up to four. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 269–283. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[13] Noam D. Elkies. Rational points near curves and small nonzero $| x^3 - y^2 |$ via lattice reduction. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 33–63. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[14] Claus Fieker and Carsten Friedrichs. On reconstruction of algebraic numbers. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 285–296. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[15] E. Victor Flynn. Coverings of curves of genus 2. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 65–84. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[16] William F. Galway. Dissecting a sieve to cut its need for space. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 297–312. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[17] Pierrick Gaudry and Robert Harley. Counting points on hyperelliptic curves over finite fields. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000*

(Leiden, The Netherlands, July 2-7, 2000), volume 1838 of *LNCS*, pages 313–332. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[18] Paul E. Gunnells. Modular symbols and hecke operators. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 347–357. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[19] Ryuichi Harasawa and Joe Suzuki. Fast jacobian group arithmetic on c_{ab} curves. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 359–376. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[20] Ming-Deh A. Huang, Ka Lam Kueh, and Ki-Seng Tan. Lifting elliptic curves and solving the elliptic curve discrete logarithm problem. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 377–384. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[21] Antoine Joux. A one round protocol for tripartite diffie-hellman. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 385–393. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[22] David R. Kohel and Igor E. Shparlinski. On exponential sums and group generators for elliptic curves over finite fields. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 395–404. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[23] David R. Kohel and William A. Stein. Component groups of quotients of $j_0(n)$. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 405–412. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[24] Stéphane Louboutin. Fast computation of relative class numbers of cm-fields. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 413–422. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[25] Siguna Müller. On probable prime testing and the computation of square roots mod n. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 423–437. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[26] Koh-ichi Nagao. Improving group law algorithms for jacobians of hyperelliptic curves. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 439–447. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[27] Phong Q. Nguyen and Jacques Stern. Lattice reduction in cryptology: An update. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 85–112. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[28] Sami Omar. Central values of artin l-functions for quaternion fields. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 449–458.

Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[29] Richard G.E. Pinch. The pseudoprimes up to 10^{13}. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 459–473. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[30] Jörg Richstein. Computing the number of goldbach partitions up to $5 \cdot 10^8$. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 474–490. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[31] Xavier-François Roblot and Brett A. Tangedal. Numerical verification of the brumer-stark conjecture. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 491–503. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[32] Fernando Rodriguez-Villegas. Explicit models of genus 2 curves with split cm. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 505–513. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[33] Renate Scheidler. Reduction in purely cubic function fields of unit rank one. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 515–532. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[34] Derek A. Smith. Factorization in the composition algebras. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on*

Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000), volume 1838 of *LNCS*, pages 533–537. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[35] Jonathan P. Sorenson. A fast algorithm for approximately counting smooth numbers. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 539–549. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[36] Roel J. Stroeker and Nikolaos Tzanakis. Computing all integer solutions of a general elliptic equation. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 551–561. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[37] Edlyn Teske and Hugh C. Williams. A note on shanks's chains of primes. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 563–580. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[38] Bert van Geemen and Jaap Top. Modular forms for gl(3) and galois representations. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 333–346. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[39] Ulrich Vollmer. Asymptotically fast discrete logarithms in quadratic number fields. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 581–594. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.

[40] André Weilert. Asymptotically fast gcd computation in $Z[i]$. In Wieb Bosma, editor, *Proceedings of the 4th International Symposium on Algorithmic Number Theory, ANTS'2000 (Leiden, The Netherlands, July 2-7, 2000)*, volume 1838 of *LNCS*, pages 595–613. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 2000.