Formal scientific papers

Daniel J. Bernstein
djb@cr.yp.to

2005.01.07

Sorted by publication date of the most recently published version. When another date is listed, it is the publication date of the first published version.

---

http://cr.yp.to/papers.html#westinghouse 21pp 1987
DJB. "New fast algorithms for π and e." Paper for the Westinghouse competition, distributed widely at the Ramanujan Centenary Conference.

---

http://cr.yp.to/papers.html#nfsi 24pp printed 1993.01
DJB, Arjen K. Lenstra. "A general number field sieve implementation." Pages 103–126 in *The development of the number field sieve*, edited by Arjen K. Lenstra, Hendrik W. Lenstra, Jr.; 3–540–57013–6, Lecture Notes in Mathematics 1554, Springer.

---

http://cr.yp.to/papers.html#231 4pp refereed printed 1994.02
DJB. "A non-iterative 2-adic statement of the $3N + 1$ conjecture." Proceedings of the American Mathematical Society **121**, 405–408.

---

http://cr.yp.to/papers.html#epsi 4pp printed 1995.05
DJB. "Enumerating and counting smooth integers." Chapter 2, Ph.D. thesis, University of California at Berkeley.

---

http://cr.yp.to/papers.html#mlnfs 5pp printed 1995.05
DJB. "The multiple-lattice number field sieve." Chapter 3, Ph.D. thesis, University of California at Berkeley.

---

http://cr.yp.to/papers.html#mmecrt 7pp printed 1995.05
DJB. "Multidigit modular multiplication with the Explicit Chinese Remainder Theorem." Chapter 4, Ph.D. thesis, University of California at Berkeley.

---

http://cr.yp.to/papers.html#fiall 8pp refereed printed 1996.06.01
DJB. "Fast ideal arithmetic via lazy localization." Pages 27–34 in *Proceedings of the Algorithmic Number Theory Symposium II*, edited by Henri Cohen; 3–540–61581–4, Lecture Notes in Computer Science 1122, Springer.

---

http://cr.yp.to/papers.html#3x1conjmap 16pp refereed printed 1996.11
DJB, Jeffrey C. Lagarias. "The $3x + 1$ conjugacy map." Canadian Journal of Mathematics **48**, 1154–1169.

---

http://cr.yp.to/papers.html#calculus 12pp 1997.04.03
DJB. "Calculus for mathematicians."

---

http://cr.yp.to/papers.html#psi-abs 3pp refereed printed 1998.07.01
DJB. "Bounding smooth integers (extended abstract)." Pages 128–130 in *Proceedings of the Algorithmic Number Theory Symposium III*, edited by Joe Buhler; 3–540–64657–4, Lecture Notes in Computer Science 1423, Springer.

http://cr.yp.to/papers.html#powers 31pp 1995.05 refereed printed 1998.07
DJB. "Detecting perfect powers in essentially linear time." Mathematics of Computation **67**, 1253–1283.

---

http://cr.yp.to/papers.html#compose 3pp refereed printed 1998.09
DJB. "Composing power series over a finite ring in essentially linear time." Journal of Symbolic Computation **26**, 339–341.

---

http://cr.yp.to/papers.html#stretch 8pp refereed printed 1999
DJB. "How to stretch random functions: the security of protected counter sums." Journal of Cryptology **12**, 185–192.

---

http://cr.yp.to/papers.html#unipat 6pp 2000.08.06
DJB. "A simple universal pattern-matching automaton."

---

http://cr.yp.to/papers.html#sigs 11pp refereed 2000.08.09
DJB. "A secure public-key signature system with extremely fast verification." Accepted to Journal of Cryptology, but withdrawn to be incorporated into author's *High-speed cryptography* book.

---

http://cr.yp.to/papers.html#sortedsums 6pp 1998.06.29 refereed printed 2001.01
DJB. "Enumerating solutions to $p(a) + q(b) = r(c) + s(d)$." Mathematics of Computation **70**, 389–394.

---

http://cr.yp.to/papers.html#m3 19pp refereed 2001.08.11
DJB. "Multidigit multiplication for mathematicians." Accepted to Advances in Applied Mathematics, but withdrawn because of incompetent printer.

---

http://cr.yp.to/papers.html#nfscircuit 11pp 2001.11.09
DJB. "Circuits for integer factorization: a proposal." Excerpted from DMS–0140542 grant proposal.

---

http://cr.yp.to/papers.html#sqroot 10pp 2001.11.23
DJB. "Faster square roots in annoying finite fields." To be incorporated into author's *High-speed cryptography* book.

---

http://cr.yp.to/papers.html#nonsquare 3pp 2001.12.20
DJB. "Faster algorithms to find non-squares modulo worst-case integers."

---

http://cr.yp.to/papers.html#pippenger 21pp 2001.12.18 2002.01.18
DJB. "Pippenger's exponentiation algorithm." To be incorporated into author's *High-speed cryptography* book.

---

http://cr.yp.to/papers.html#sf 15pp 2000.06.22 2002.09.23
DJB. "How to find small factors of integers." Now being revamped in light of `smoothparts` results.

---

http://cr.yp.to/papers.html#psi 18pp 2000.11.03 refereed printed 2002.10.01
DJB. "Arbitrarily tight bounds on the distribution of smooth integers." Pages 49–66 in *Number theory for the Millennium I*, edited by Michael A. Bennett, Bruce C. Berndt, Nigel Boston, Harold G. Diamond, Adolf J. Hildebrand, Walter Philipp; 1–56881–146–2, A. K. Peters.

`http://cr.yp.to/papers.html#aks` 15pp 2002.08.09 2003.01.25
DJB. “Proving primality after Agrawal-Kayal-Saxena.”

`http://cr.yp.to/papers.html#logfloor` 4pp 2003.06.29 2003.06.30
DJB. “Computing logarithm floors in essentially linear time.”

`http://cr.yp.to/papers.html#logagm` 8pp 2003.07.17 2003.07.17
DJB. “Computing logarithm intervals with the arithmetic-geometric-mean iteration.”

`http://cr.yp.to/papers.html#meecrt` 11pp 2003.08.15 2003.08.15
DJB, Jonathan P. Sorenson. “Modular exponentiation via the explicit Chinese remainder theorem.”

`http://cr.yp.to/papers.html#rwtight` 13pp 2003.09.26 2003.09.26
DJB. “Proving tight security for standard Rabin-Williams signatures.” To be incorporated into author’s *High-speed cryptography* book.

`http://cr.yp.to/papers.html#abccong` 5pp 2003.03.14 refereed 2004.02.10
DJB. “Sharper ABC-based bounds for congruent polynomials.” To be printed in Journal de Théorie des Nombres de Bordeaux.

`http://cr.yp.to/papers.html#smallheight` 13pp 2003.09.18 refereed 2004.02.10
DJB. “Reducing lattice bases to find small-height values of univariate polynomials.” To be printed in *Algorithmic number theory*, edited by Joe Buhler, Peter Stevenhagen.

`http://cr.yp.to/papers.html#fastnewton` 13pp 1998.06.27 2004.03.09
DJB. “Removing redundancy in high-precision Newton iteration.”

`http://cr.yp.to/papers.html#primesieves` 8pp 1999.05.05 refereed printed 2004.04
A. O. L. Atkin, DJB. “Prime sieves using binary quadratic forms.” Mathematics of Computation **73**, 1023–1030.

`http://cr.yp.to/papers.html#smoothparts` 7pp 2004.05.10 2004.05.10
DJB. “How to find smooth parts of integers.”

`http://cr.yp.to/papers.html#focus` 8pp 2001.12.31 refereed printed 2004.06.10
DJB. “Doubly focused enumeration of locally square polynomial values.” Pages 69–76 in *High primes and misdemeanours*, edited by Alf van der Poorten, Andreas Stein; 0–8218–3353–7, American Mathematical Society.

`http://cr.yp.to/papers.html#powers2` 3pp 2004.06.30 2004.06.30
DJB, Hendrik W. Lenstra, Jr., Jonathan Pila. “Detecting perfect powers by factoring into coprimes.”

`http://cr.yp.to/papers.html#scaledmod` 8pp 2004.08.20 2004.08.20
DJB. “Scaled remainder trees.”

`http://cr.yp.to/papers.html#forgery` 10pp 2001.07.31 refereed 2004.09.06
DJB. “Protecting communications against forgery.” To be printed in *Algorithmic number theory*, edited by Joe Buhler, Peter Stevenhagen.

`http://cr.yp.to/papers.html#hash127` 21pp 1999.04.04 2004.09.18
DJB. “Floating-point arithmetic and message authentication.” To be incorporated into author’s *High-speed cryptography* book.

`http://cr.yp.to/papers.html#multapps` 47pp 2003.01.19 refereed 2004.10.07
DJB. "Fast multiplication and its applications." To be printed in *Algorithmic number theory*, edited by Joe Buhler, Peter Stevenhagen.

`http://cr.yp.to/papers.html#securitywcs` 10pp 2004.10.19 2004.10.27
DJB. "Stronger security bounds for Wegman-Carter-Shoup authenticators."

`http://cr.yp.to/papers.html#poly1305` 17pp 2004.11.01 2004.11.01
DJB. "The Poly1305-AES message-authentication code."

`http://cr.yp.to/papers.html#dcba2` 4pp 2004.10.09 2004.11.03
DJB. "Research announcement: Faster factorization into coprimes."

`http://cr.yp.to/papers.html#cachetiming` 12pp 2004.11.11 2004.11.21
DJB. "Cache-timing attacks on AES."

`http://cr.yp.to/papers.html#quartic` 15pp 2003.01.28 2004.12.03
DJB. "Proving primality in essentially quartic random time."

`http://cr.yp.to/papers.html#prime2004` 15pp 2004.02.12 2004.12.23
DJB. "Distinguishing prime numbers from composite numbers: the state of the art in 2004."

`http://cr.yp.to/papers.html#dcba` 30pp 1996.05.12 refereed printed 2005.01
DJB. "Factoring into coprimes in essentially linear time." Journal of Algorithms **54**, 1–30.