List of publications

Daniel J. Bernstein
djb@cr.yp.to

2008.09.17

This is a list of formal scientific papers, 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.

This list does not include other publications, such as software; see my web page http://cr.yp.to.

---

http://cr.yp.to/papers.html#westinghouse 21pp 1987
DJB. "New fast algorithms for π and e." Fifth-place paper for the nationwide 1987 Westinghouse Science Talent Search. 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. Lecture Notes in Mathematics **1554**, Springer, 1993. ISBN 3–540–57013–6.

---

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** (1994), 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. Lecture Notes in Computer Science **1122**, Springer, 1996. ISBN 3–540–61581–4.

---

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** (1996), 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. Lecture Notes in Computer Science **1423**, Springer, 1998. ISBN 3–540–64657–4.

---

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** (1998), 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** (1998), 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** (1999), 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** (2001), 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 by author to prevent irreparable mangling by Academic Press.

`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. A. K. Peters, 2002. ISBN 1–56881–146–2.

`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#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** (2004), 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. Fields Institute Communications **41**, American Mathematical Society, 2004. ISBN 0–8218–3353–7.

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

`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#dcba2` 4pp 2004.10.09 2004.11.03
DJB. "Research announcement: Faster factorization into coprimes."

`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** (2005), 1–30.

`http://cr.yp.to/papers.html#easycbc` 6pp 2005.01.09 2005.01.09
DJB. "A short proof of the unpredictability of cipher block chaining."

`http://cr.yp.to/papers.html#securitywcs` 17pp 2004.10.19 refereed printed 2005.02.27
DJB. "Stronger security bounds for Wegman-Carter-Shoup authenticators." Pages 164–180 in *Advances in Cryptology: EUROCRYPT 2005*, edited by Ronald Cramer. Lecture Notes in Computer Science **3494**, Springer, 2005. ISBN 3–540–25910–4.

`http://cr.yp.to/papers.html#permutations` 10pp 2005.03.23 2005.03.23
DJB. "Stronger security bounds for permutations." To be incorporated into author's *High-speed cryptography* book.

`http://cr.yp.to/papers.html#poly1305` 18pp 2004.11.01 refereed printed 2005.03.29
DJB. "The Poly1305-AES message-authentication code." Pages 32–49 in *Proceedings of FSE 2005*, edited by H. Gilbert and H. Handschuh. Lecture Notes in Computer Science **3557**, Springer, 2005. ISBN 3–540–26541–4.

`http://cr.yp.to/papers.html#cachetiming` 37pp 2004.11.11 2005.04.14
DJB. "Cache-timing attacks on AES."

`http://cr.yp.to/papers.html#bruteforce` 10pp 2005.04.25 refereed 2005.04.25
DJB. "Understanding brute force." ECRYPT STVL Workshop on Symmetric Key Encryption.

`http://cr.yp.to/papers.html#abccong` 5pp 2003.03.14 refereed printed 2005.12.24
DJB. "Sharper ABC-based bounds for congruent polynomials." Journal de Theorie des Nombres de Bordeaux **17** (2005), 721–725.

`http://cr.yp.to/papers.html#stream256` 14pp 2005.12.23 refereed 2006.01.23
DJB. "Comparison of 256-bit stream ciphers at the beginning of 2006." SASC 2006: Stream Ciphers Revisited.

`http://cr.yp.to/papers.html#curve25519` 22pp 2005.11.15 refereed printed 2006.02.09
DJB. "Curve25519: new Diffie-Hellman speed records." Pages 207–228 in *Proceedings of PKC 2006*, edited by Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin. Lecture Notes in Computer Science **3958**, Springer, 2006. ISBN 3–540–33851–9.

`http://cr.yp.to/papers.html#diffchain` 16pp 2006.02.19 2006.02.19
DJB. "Differential addition chains."

`http://cr.yp.to/papers.html#zkcrypt` 4pp 2006.03.02 2006.03.02
DJB. "Does ZK-Crypt version 1 flunk a repetition test?"

`http://cr.yp.to/papers.html#curvezero` 13pp 2006.07.21 2006.07.26
DJB. "Can we avoid tests for zero in fast elliptic-curve arithmetic?"

`http://cr.yp.to/papers.html#quartic` 15pp 2003.01.28 refereed printed 2006.09.14
DJB. "Proving primality in essentially quartic random time." Mathematics of Computation **76** (2007), 389–403.

`http://cr.yp.to/papers.html#meecrt` 12pp 2003.08.15 refereed printed 2006.09.14
DJB, Jonathan P. Sorenson. "Modular exponentiation via the explicit Chinese remainder theorem." Mathematics of Computation **76** (2007), 443–454.

`http://cr.yp.to/papers.html#powers2` 4pp 2004.06.30 refereed printed 2006.09.14
DJB, Hendrik W. Lenstra, Jr., Jonathan Pila. "Detecting perfect powers by factoring into coprimes." Mathematics of Computation **76** (2007), 385–388.

`http://cr.yp.to/papers.html#kdvseries` 4pp 2006.10.19 2006.10.19
DJB. "Using fast power-series arithmetic in the Kedlaya-Denef-Vercauteren algorithm."

`http://cr.yp.to/papers.html#aecycles` 13pp 2007.01.11 refereed 2007.01.18
DJB. "Cycle counts for authenticated encryption." Workshop Record of SASC 2007: The State of the Art of Stream Ciphers.

`http://cr.yp.to/papers.html#expandxor` 10pp 2007.04.11 refereed 2007.05.03
DJB. "What output size resists collisions in a xor of independent expansions?" Workshop Record of ECRYPT Workshop on Hash Functions 2007.

`http://cr.yp.to/papers.html#cipherdag` 2pp 2007.06.30 refereed 2007.06.30
DJB. "Cipher DAGs." Workshop Record of ECRYPT Workshop on Tools for Cryptanalysis.

`http://cr.yp.to/papers.html#antiquad` 19pp 2007.03.03 refereed printed 2007.08.17
Bo-Yin Yang, Owen Chia-Hsin Chen, DJB, Jiun-Ming Chen. "Analysis of QUAD." Pages 290–308 in *Fast Software Encryption, 14th International Workshop, FSE 2007*, edited by Alex Biryukov. Lecture Notes in Computer Science **4593**, Springer, 2007. ISBN 978–3-540–74617–1.

`http://cr.yp.to/papers.html#genbday` 8pp 2007.07.19 refereed 2007.09.04
DJB. "Better price-performance ratios for generalized birthday attacks." Workshop Record of SHARCS'07: Special-purpose Hardware for Attacking Cryptographic Systems.

`http://cr.yp.to/papers.html#newelliptic` 20pp 2007.04.10 refereed printed 2007.09.06
DJB, Tanja Lange. "Faster addition and doubling on elliptic curves." *Advances in Cryptology: ASIACRYPT 2007*, edited by Kaoru Kurosawa. Lecture Notes in Computer Science **4833**, Springer, 2007. ISBN 978–3-540–76899–9.

`http://cr.yp.to/papers.html#tangentfft` 10pp 2007.08.09 refereed printed 2007.09.19
DJB. "The tangent FFT." Pages 291–300 in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium, AAECC–17, Bangalore, India, December 16–20, 2007, Proceedings*, edited by Serdar Boztas and Hsiao-feng Lu, Lecture Notes in Computer Science **4851**, Springer, 2007. ISBN 978–3-540–77223–1.

`http://cr.yp.to/papers.html#inverted` 8pp 2007.10.09 printed 2007.10.09
DJB, Tanja Lange. "Inverted Edwards coordinates." Pages 20–27 in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium, AAECC–17, Bangalore, India, December 16–20, 2007, Proceedings*, edited by Serdar Boztas and Hsiao-feng Lu, Lecture Notes in Computer Science **4851**, Springer, 2007. ISBN 978–3-540–77223–1. Paper invited from Lange by conference organizers.

`http://cr.yp.to/papers.html#pema` 14pp 2007.10.22 2007.10.22
DJB. "Polynomial evaluation and message authentication."

`http://cr.yp.to/papers.html#doublebase` 16pp 2007.10.28 refereed printed 2007.10.28
DJB, Peter Birkner, Tanja Lange, Christiane Peters. "Optimizing double-base elliptic-curve single-scalar multiplication." *Progress in Cryptology: INDOCRYPT 2007*, edited by Kannan Srinathan, Chandrasekaran Pandu Rangan, and Moti Yung. Lecture Notes in Computer Science **4859**, Springer, 2007. ISBN 978–3-540–77025–1.

`http://cr.yp.to/papers.html#qmailsec` 10pp 2007.11.01 printed 2007.11.01
DJB. "Some thoughts on security after ten years of qmail 1.0." Computer Security Architecture Workshop (CSAW). Paper invited by conference organizers.

`http://cr.yp.to/papers.html#efd` 19pp 2007.12.04 refereed printed 2007.12.04
DJB, Tanja Lange. "Analysis and optimization of elliptic-curve single-scalar multiplication." Pages 1–19 in *Finite fields and applications: proceedings of Fq8*, edited by Gary L. Mullen, Daniel Panario, and Igor E. Shparlinski, Contemporary Mathematics **461**, American Mathematical Society, 2008. ISBN 978–0-8218–4309–3.

`http://cr.yp.to/papers.html#salsafamily` 15pp 2007.12.25 printed 2007.12.25
DJB. "The Salsa20 family of stream ciphers." Pages 84–97 in *New stream cipher designs: the eSTREAM finalists*, edited by Matthew Robshaw and Olivier Billet, Lecture Notes in Computer Science **4986**, Springer, 2008. ISBN 978–3-540–68350–6. Paper invited by book editors.

`http://cr.yp.to/papers.html#eecm` 16pp 2008.01.09 2008.01.20
DJB, Peter Birkner, Tanja Lange, Christiane Peters. "ECM using Edwards curves."

`http://cr.yp.to/papers.html#chacha` 6pp 2008.01.20 refereed 2008.01.28
DJB. "ChaCha, a variant of Salsa20." Workshop Record of SASC 2008: The State of the Art of Stream Ciphers.

`http://cr.yp.to/papers.html#rwsota` 11pp 2008.01.31 2008.01.31
DJB. "RSA signatures and Rabin-Williams signatures: the state of the art."

`http://cr.yp.to/papers.html#rwtight` 18pp 2003.09.26 refereed printed 2008.02.01
DJB. "Proving tight security for Rabin-Williams signatures." Pages 70–87 in *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13–17, 2008, Proceedings*, edited by Nigel Smart, Lecture Notes in Computer Science **4965**, Springer, 2008. ISBN 978–3-540–78966–6.

`http://cr.yp.to/papers.html#twisted` 17pp 2008.01.08 refereed printed 2008.03.13
DJB, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters. "Twisted Edwards curves." Pages 389–405 in *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11–14, 2008, Proceedings*, edited by Serge Vaudenay, Lecture Notes in Computer Science **5023**, Springer, 2008. ISBN 978–3-540–68159–5.

`http://cr.yp.to/papers.html#broken` 35pp 2008.02.21 2008.03.30
DJB. "Which eSTREAM ciphers have been broken?"

`http://cr.yp.to/papers.html#phase3speed` 13pp 2008.02.25 2008.03.31
DJB. "Which phase–3 eSTREAM ciphers provide the best software speeds?"

`http://cr.yp.to/papers.html#forgery` 15pp 2001.07.31 refereed 2008.05.01
DJB. "Protecting communications against forgery." To be printed in *Algorithmic number theory*, edited by Joe Buhler, Peter Stevenhagen. Cambridge University Press. ISBN 978–0521808545.

`http://cr.yp.to/papers.html#smallheight` 26pp 2003.09.18 refereed 2008.05.02
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. Cambridge University Press. ISBN 978–0521808545.

`http://cr.yp.to/papers.html#multapps` 60pp 2003.01.19 refereed 2008.05.15
DJB. "Fast multiplication and its applications." To be printed in *Algorithmic number theory*, edited by Joe Buhler, Peter Stevenhagen. Cambridge University Press. ISBN 978–0521808545.

`http://cr.yp.to/papers.html#edwards2` 23pp 2008.04.15 refereed printed 2008.06.11
DJB, Tanja Lange, Reza Rezaeian Farashahi. "Binary Edwards curves." Pages 244–265 in *Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10–13, 2008, Proceedings*, edited by Elisabeth Oswald and Pankaj Rohatgi, Lecture Notes in Computer Science **5154**, Springer, 2008. ISBN 978–3-540–85052–6.

`http://cr.yp.to/papers.html#goppalist` 16pp 2008.07.06 2008.07.06
DJB. "List decoding for binary Goppa codes."

`http://cr.yp.to/papers.html#mceliece` 16pp 2008.07.22 refereed 2008.08.07
DJB, Tanja Lange, Christiane Peters. "Attacking and defending the McEliece cryptosystem." To be printed in Proceedings of PQCrypto 2008. Springer.

`http://cr.yp.to/papers.html#aesspeed` 18pp 2008.09.08 refereed 2008.09.08
DJB, Peter Schwabe. "New AES software speed records." To be printed in Proceedings of Indocrypt 2008. Springer.