Bibliography of Benne de Weger, August 22, 2019

A Dutch flag indicates a publication in Dutch.
A British flag indicates a publication in English.
A link symbol indicates a URL, from where the publication can be downloaded.

Theses

Benne de Weger,
Over p-adische benaderingen,
Doctoraalscriptie (Master Thesis), Universiteit Leiden, 1983.
http://www.win.tue.nl/~bdeweger/scriptie.html

Benne de Weger,
Algorithms for Diophantine equations,
PhD Thesis (proefschrift), University of Leiden, 1988.
http://www.win.tue.nl/~bdeweger/proefschrift.html

Books

Benne de Weger,
Algorithms for Diophantine equations,
CWI Tract 65, Centrum voor Wiskunde en Informatica, Amsterdam, 1989, ISBN 9061963753, MR 90m:11205.
▷ This is a slightly updated version of my PhD Thesis. It is out of print, but both CWI and I have put it online:
http://oai.cwi.nl/oai/asset/13190/13190A.pdf,
http://www.win.tue.nl/~bdeweger/downloads/CWI%20Tract%2065.pdf.

Benne de Weger,
Elementaire Getaltheorie en Asymmetrische Cryptografie,
Epsilon Uitgaven, deel 63, Utrecht, 2009, ISBN 9789050411080.
http://www.win.tue.nl/~bdeweger/epsilonboek.html.
▷ 2e druk, 2011, 3e druk, 2016.

Scientific papers

[1] B.M.M. de Weger,
"Approximation lattices of p-adic numbers",
Journal of Number Theory **24**(1) [1986], 70–88, MR 87k:11069.
http://deweger.xs4all.nl/papers/[1]dW-ApprLatt-JNumTh[1986].pdf.

[2] A. Pethő and B.M.M. de Weger,
"Products of prime powers in binary recurrence sequences I. The hyperbolic case, with an application to the generalized Ramanujan-Nagell equation",
Mathematics of Computation **47**(176) [1986], 713–727, MR 87m:11027a.
http://deweger.xs4all.nl/papers/[2]PtdW-PowRecI-MathComp[1986].pdf.

[3] B.M.M. de Weger,
"Products of prime powers in binary recurrence sequences II. The elliptic case, with an application to a mixed quadratic-exponential equation",
Mathematics of Computation **47**(176) [1986], 729–739, MR 87m:11027b.
http://deweger.xs4all.nl/papers/[3]dW-PowRecII-MathComp[1986].pdf.

[4] B.M.M. de Weger,
"Solving exponential Diophantine equations using lattice basis reduction algorithms",
Journal of Number Theory **26**(3) [1987], 325–367, MR 88k:11097.
http://deweger.xs4all.nl/papers/[4]dW-ExpDio-JNumTh[1987].pdf.
▷ Erratum: *Journal of Number Theory* **31**(1) [1989], 88–89, MR 90a:11040.
http://deweger.xs4all.nl/papers/[4a]dW-ExpDio-errat-JNumTh[1987].pdf.

[5] B.M.M. de Weger,
"Periodicity of p-adic continued fractions",
Elemente der Mathematik **43**(4) [1988], 112–116, MR 89j:11006.
http://deweger.xs4all.nl/papers/[5]dW-PerContFr-ElemMat[1988].pdf.

[6] N. Tzanakis and B.M.M. de Weger,
"On the practical solution of the Thue equation",
Journal of Number Theory **31**(2) [1989], 99–132, MR 90c:11018.
http://deweger.xs4all.nl/papers/[6]TzdW-Thue-JNumTh[1989].pdf.

[7] B.M.M. de Weger,
"A Diophantine equation of Antoniadis",
in: R.A. Mollin (ed.), *Number Theory and Applications*, NATO Advanced Science Institutes Series C: Mathematical and Physical Sciences, Vol. 265, Kluwer, Dordrecht, 1989, pp. 575–589, MR 92f:11048.
http://deweger.xs4all.nl/papers/[7]dW-Ant-NATO[1989].pdf.

[8] B.M.M. de Weger,
"On the practical solution of Thue-Mahler equations, an outline",
in: K. Győry and G. Halász (eds.), *Number Theory*, Colloq. Math. Soc. János Bolyai, Vol. 51, North-Holland, Amsterdam, 1990, pp. 1037–1050, MR 91f:11092.
http://deweger.xs4all.nl/papers/[8]dW-ThMahlOutl-Bolyai[1990].pdf.

[9] B.M.M. de Weger,
"The weighted sum of two S-units being a square",
Indagationes Mathematicae (New Series), **1**(2) [1990], 243–262, MR 91j:11017.
http://deweger.xs4all.nl/papers/[9]dW-SumSUn-Indag[1990].pdf.

[10] N. Tzanakis and B.M.M. de Weger,
"Solving a specific Thue-Mahler equation",
Mathematics of Computation **57**(196) [1991], 799–815, MR 92a:11028.
http://deweger.xs4all.nl/papers/[10]TzdW-SpThueMahl-MathComp[1991].pdf.

[11] N. Tzanakis and B.M.M. de Weger,
"On the practical solution of the Thue-Mahler equation",
in: A. Pethö, M.E. Pohst, H.C. Williams and H.G. Zimmer (eds.), *Computational number theory, Proc. Colloq. Debrecen 1989*, De Gruyter, Berlin, 1991, pp. 289–294, MR 93a:11026.
http://deweger.xs4all.nl/papers/[11]TzdW-ThueMahl-Debr[1991].pdf.

[12] B.M.M. de Weger,
"A hyperelliptic Diophantine equation related to imaginary quadratic number fields with class number 2",
Journal für die Reine und Angewandte Mathematik **427** [1992], 137–156, MR 93d:11034.
http://deweger.xs4all.nl/papers/[12]dW-HypEll-Crelle[1992].pdf.
▷ Correction: *Journal für die Reine und Angewandte Mathematik* **441** [1993], 217–218, MR 94h:11026.
http://deweger.xs4all.nl/papers/[12a]dW-HypEll-corr-Crelle[1992].pdf.

[13] N. Tzanakis and B.M.M. de Weger,
"How to explicitly solve a Thue-Mahler equation",
Compositio Mathematica **84**(3) [1992], 223–288, MR 93k:11025.
http://deweger.xs4all.nl/papers/[13]TzdW-ThueMahl-Comp[1992].pdf.
▷ Correction: *Compositio Mathematica* **89**(2) [1993], 241–242, MR 95a:11030.
http://deweger.xs4all.nl/papers/[13a]TzdW-ThueMahl-corr-Comp[1992].pdf.

[14] Roel J. Stroeker and Benjamin M.M. de Weger,
"On elliptic Diophantine equations that defy Thue's method: the case of the Ochoa curve",
Experimental Mathematics **3**(3) [1994], 209–220, MR 96c:11033.
http://deweger.xs4all.nl/papers/[14]StdW-Ochoa-ExpMath[1994].pdf.

[15] B.M.M. de Weger,
"A Thue equation with quadratic integers as variables",
Mathematics of Computation **64**(210) [1995], 855–861, MR 95f:11020.
http://deweger.xs4all.nl/papers/[15]dW-ThueQuad-MathComp[1995].pdf.

[16] B.M.M. de Weger,
"A curious property of the eleventh Fibonacci number",
Rocky Mountain Journal of Mathematics **25**(3) [1995], 977–994, MR 96k:11017.
http://deweger.xs4all.nl/papers/[16]dW-11Fib-RockMtn[1995].pdf.

[17] Maurice Mignotte and Benjamin M.M. de Weger,
"On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$",
Glasgow Mathematical Journal **38**(1) [1996], 77–85, MR 97b:11044.
http://deweger.xs4all.nl/papers/[17]MidW-Dio-GlasgMJ[1996].pdf.

[18] Roel J. Stroeker and Benjamin M.M. de Weger,
"On a quartic Diophantine equation",
Proceedings of the Edinburgh Mathematical Society, Series II **39**(1) [1996], 97–114, MR 97c:11039.
http://deweger.xs4all.nl/papers/[18]StdW-Quartic-PrEdinbMS[1996].pdf.

[19] B.M.M. de Weger,
"A binomial Diophantine equation",
Quarterly Journal of Mathematics, Oxford, Second Series **47**(186) [1996], 221–231, MR 97c:11041.
http://deweger.xs4all.nl/papers/[19]dW-BinomDio-QuJMathOxf[1996].pdf.

[20] Benjamin M.M. de Weger,
"Equal binomial coefficients: some elementary considerations",
Journal of Number Theory **63**(2) [1997], 373–386, MR 98b:11027.
http://deweger.xs4all.nl/papers/[20]dW-EqBinom-JNumTh[1997].pdf.

[21] Benjamin M.M. de Weger,
"Padua and Pisa are exponentially far apart",
Publicacions Matemàtiques (Barcelona) **41**(2) [1997], 631–651, MR 98j:11009.
http://deweger.xs4all.nl/papers/[21]dW-PadPis-PubMatBarc[1997].pdf.

[22] Ákos Pintér and Benjamin M.M. de Weger,
"$210 = 14 \times 15 = 5 \times 6 \times 7 = \binom{21}{2} = \binom{10}{4}$",
Publicationes Mathematicae Debrecen **51**(1–2) [1997], 175–189, MR 98k:11032.
http://deweger.xs4all.nl/papers/[22]PidW-210-PubMatDebr[1997].pdf.

[23] B.M.M. de Weger,
"S-integral solutions to a Weierstrass equation",
Journal de Théorie des Nombres de Bordeaux **9**(2) [1997], 281–301, MR 99d:11027.
http://deweger.xs4all.nl/papers/[23]dW-SInt-JThNomBord[1997].pdf.

[24] Michael A. Bennett and Benjamin M.M. de Weger,
"On the Diophantine equation $|ax^n - by^n| = 1$",
Mathematics of Computation **67**(221) [1998], 413–438, MR 98c:11024.
http://deweger.xs4all.nl/papers/[24]BndW-axby-MatComp[1998].pdf.

[25] Benjamin M.M. de Weger,
'$A + B = C$ and big Ш's",
Quarterly Journal of Mathematics, Oxford, Second Series **49**(193) [1998], 105–128, MR 99j:11065.
http://deweger.xs4all.nl/papers/[25]dW-ABCSha-QuJMathOxf[1998].pdf.

[26] Benjamin M.M. de Weger,
"On the fourth-powerfree part of $x^2 + 2$",
Glasgow Mathematical Journal **40**(3) [1998], 299–310, MR 99k:11045.
http://deweger.xs4all.nl/papers/[26]dW-Fourth-GlssgMJ[1998].pdf.

[27] Benjamin M.M. de Weger,
"Solving elliptic Diophantine equations avoiding Thue equations and elliptic logarithms",
Experimental Mathematics **7**(3) [1998], 243–256, MR 99m:11148.
http://deweger.xs4all.nl/papers/[27]dW-EllAvoidThue-ExpMath[1998].pdf.

[28] Roelof J. Stroeker and Benjamin M.M. de Weger,
"Elliptic binomial Diophantine equations",
Mathematics of Computation **68**(227) [1999], 1257–1281, MR 99i:11122.
http://deweger.xs4all.nl/papers/[28]StdW-EllBinom-MathComp[1999].pdf.

[29] Roelof J. Stroeker and Benjamin M.M. de Weger,
"Solving elliptic Diophantine equations: the general cubic case",
Acta Arithmetica **87**(4) [1999], 339–365, MR 99m:11029.
http://deweger.xs4all.nl/papers/[29]StdW-EllCubic-ActaArith[1999].pdf.

[30] B.M.M. de Weger and C.E. van de Woestijne,
"On the diameter of sets of almost powers",
Acta Arithmetica **90**(4) [1999], 371–385, MR 2000j:11109.
http://deweger.xs4all.nl/papers/[30]vdWdW-DiamCons-ActaArith[1999].pdf.

[31] B.M.M. de Weger and C.E. van de Woestijne,
"On the power-free parts of consecutive integers",
Acta Arithmetica **90**(4) [1999], 387–395, MR 2000i:11145.
http://deweger.xs4all.nl/papers/[31]vdWdW-PowFree-ActaArith[1999].pdf.

[32] Roelof J. Stroeker and Benjamin M.M. de Weger,
"On integral zeroes of binary Krawtchouk polynomials",
Nieuw Archief voor Wiskunde, Vierde Serie **17**(2) [1999], 175–186, MR 2000k:33029.
http://deweger.xs4all.nl/papers/[32]StdW-Kraw-NAvW[1999].pdf.
▷ Reprinted in: Nina Virchenko, Ivan Katchanovski, Viktor Haidey, Roman Andrushkiw, Roman Voronka (eds.), *Development of the mathematical ideas of Mykhailo Kravchuk (Krawtchouk)*, Shevchenko Scientific Society (USA), National Technical University of Ukraine "KPI", New York, Kyiv, 2004, pp. 623–633.

[33] Benne de Weger,
"Cryptanalysis of RSA with small prime difference",
Applicable Algebra in Engineering, Communication and Computing **13**(1) [2002], 17–28, MR 2003j:94088.
http://deweger.xs4all.nl/papers/[33]dW-SmlPrDif-AAECC[2002].pdf.

[34] John Simons and Benne de Weger,
"Mersenne en het Syracuseprobleem",
Nieuw Archief voor Wiskunde, Vijfde Serie **5**(3) [2004], 218–220.
http://deweger.xs4all.nl/papers/[34]SidW-MersSyrac-NwArch[2004].pdf.

[35] John Simons and Benne de Weger,
"Theoretical and computational bounds for m-cycles of the $3n+1$-problem",
Acta Arithmetica **117**(1) [2005], 51–70, MR 2005h:11049.
http://deweger.xs4all.nl/papers/[35]SidW-3n+1-ActaArith[2005].pdf.
▷ An updated version:
http://deweger.xs4all.nl/papers/[35a]SidW-3n+1-v1.44[2010].pdf.

[36] Matthias Ernst, Ellen Jochemsz, Alexander May and Benne de Weger,
"Partial Key Exposure Attacks on RSA Up to Full Size Exponents",
in: R. Cramer (ed.), *Advances in Cryptology - EUROCRYPT 2005*, Lecture Notes in Computer Science Vol. 3494, Springer, Berlin, 2005, pp. 371–386, MR 2008h:94057.
http://deweger.xs4all.nl/papers/[36]ErJoMadW-PartKeyExp-EuroCrypt[2005].pdf.

[37] Arjen Lenstra and Benne de Weger,
"On the Possibility of Constructing Meaningful Hash Collisions for Public Keys",
in: C. Boyd and J.M. González Nieto, *Information Security and Privacy, Proceedings ACISP 2005*, Lecture Notes in Computer Science Vol. 3574, Springer, Berlin, 2005, pp. 267–279.
http://deweger.xs4all.nl/papers/[37]LedW-X509-ACISP[2005].pdf.
▷ Full version (including an appendix co-authored by Xiaoyun Wang) is available online:
http://deweger.xs4all.nl/papers/[37a]LedW-X509-full-web[2005].pdf.

[38] Arjen K. Lenstra and Benjamin M.M. de Weger,
"Twin RSA",
in: E. Dawson and S. Vaudenay (eds.), *Progress in Cryptology - MyCrypt 2005*, Lecture Notes in Computer Science Vol. 3715, Springer, Berlin, 2005, pp. 222-228.
http://deweger.xs4all.nl/papers/[38]LedW-TwinRSA-MyCrypt[2005].pdf.

[39] Ellen Jochemsz and Benne de Weger,
"A Partial Key Exposure Attack on RSA Using a 2-Dimensional Lattice",
in: S.K. Katsikas, J. Lopez, M. Backes, S. Gritzalis and B. Preneel (eds.), *Information Security, Proceedings ISC 2006*, Lecture Notes in Computer Science Vol. 4176, Springer, Berlin, 2006, pp. 203-216.
http://deweger.xs4all.nl/papers/[39]JodW-PartKeyExp2Dim-ISC[2006].pdf.

[40] Marc Stevens, Arjen Lenstra and Benne de Weger,
"Chosen-prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities",
in: Moni Naor (ed.), *Advances in Cryptology - EUROCRYPT 2007*, Lecture Notes in Computer Science Vol. 4515, Springer, Berlin, 2007, pp. 1–22.
http://deweger.xs4all.nl/papers/[40]StLedW-ChosPref-EuroCrypt[2007].pdf.

[41] Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik and Benne de Weger,
"Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate",
in: Shai Halevi (ed.), *Advances in Cryptology - CRYPTO 2009*, Lecture Notes in Computer Science Vol. 5677, Springer, Berlin, 2009, pp. 55–69.
http://deweger.xs4all.nl/papers/[41]StSoApLeMoOsdW-RogueCA-Crypto[2009].pdf.

[42] Marc Stevens, Arjen Lenstra and Benne de Weger,
"Chosen-prefix Collisions for MD5 and Applications",
International Journal of Applied Cryptography **2** No. 4 [2012], 322–359.
http://deweger.xs4all.nl/papers/[42]StLedW-MD5-IJACT[2012].pdf.

[43] Florian Luca, Pieter Moree and Benne de Weger,
"Some Diophantine equations from finite group theory: $\Phi_m(x) = 2p^n - 1$",
Publicationes Mathematicae Debrecen **78/2** [2011], 377–392,
http://deweger.xs4all.nl/papers/[43]LuModW-Phi-PMD[2011].pdf.
▷ Extended version: Max Planck Institute for Mathematics Preprint MPIM2009-62, 2009.
http://deweger.xs4all.nl/papers/[43a]LuModW-Phi-MPIM[2009].pdf.

[44] Meilof Veeningen, Benne de Weger and Nicola Zannone,
"Modeling identity-related properties and their privacy strength",
in P. Degano, S. Etalle and J. Guttman (eds.), *Formal Aspects of Security and Trust*, Proceedings of FAST 2010, Lecture Notes in Computer Science Vol. 6561, Springer, Berlin, 2011, pp. 126–140.
http://deweger.xs4all.nl/papers/[44]VdWZ-PImodel-FAST[2011].pdf.

[45] Florian Luca and Benne de Weger,
"$\sigma_k(F_m) = F_n$",
New Zealand Journal of Mathematics **40** [2010], 1–13.
http://deweger.xs4all.nl/papers/[45]LudW-sFmFn-NZJM[2011].pdf.

[46] Meilof Veeningen, Benne de Weger and Nicola Zannone,
"Formal Privacy Analysis of Communication Protocols for Identity Management",
in S. Jajodia and C. Mazumdar, (eds.), *Information Systems Security*, Proceedings of ICISS 2011, Kolkata, India,
Lecture Notes in Computer Science Vol. 7093, Springer, Berlin, 2011, pp. 235–249.
http://deweger.xs4all.nl/papers/[46]VdWZ-PACPIM-ICISS[2011].pdf.

[47] Thijs Laarhoven and Benne de Weger,
"Optimal symmetric Tardos traitor tracing schemes",
Designs, Codes and Cryptography **71** [2014], 83–103.
published online: July 10, 2012.
http://deweger.xs4all.nl/papers/[47]LdW-OptTTTS-DCC[2014].pdf.

[48] Thijs Laarhoven, Jeroen Doumen, Peter Roelse, Boris Škorić and Benne de Weger,
"Dynamic Tardos traitor tracing schemes",
IEEE Transactions on Information Theory **59** [2013], 4230–4242.
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6507628.

[49] Meilof Veeningen, Benne de Weger and Nicola Zannone,
"Data Minimisation in Communication Protocols: A Formal Analysis Framework and Application to Identity Management",
International Journal of Information Security **13** [2014], 529–569,
http://rd.springer.com/article/10.1007/s10207-014-0235-z.
An earlier version of this paper had the title "A Formal Privacy Analysis of Identity Management Systems".

[50] Meilof Veeningen, Benne de Weger and Nicola Zannone,
"Formal Modelling of (De)Pseudonymisation: A Case Study in Health Care Privacy",
In Audun Jøsang, Pierangela Samarati and Marinella Petrocchi (Eds.), *Security and Trust Management*, Proceedings of STM, Pisa, September 2012, Springer LNCS 7783, 2013, pp. 145–160
http://deweger.xs4all.nl/papers/[50]MdWZ-Pseudon[2012].pdf.

[51] Thijs Laarhoven and Benne de Weger,
"The Collatz conjecture and De Bruijn graphs",
Indagationes Mathematicae **24** [2013], 971-983,
http://deweger.xs4all.nl/papers/[52]LdW-CollBruijn-IndagMath[2013].pdf.

[52] Meilof Veeningen, Benne de Weger and Nicola Zannone,
"Symbolic Privacy Analysis through Linkability and Detectability",
in: Carmen Fernández-Gago, Fabio Martinelli, Siani Pearson, Isaac Agudo (Eds), *Trust Management VII*, IFIP Advances in Information and Communication Technology Vol. 401, 2013, Proceedings of the 7th IFIP WG 11.11 International Conference, IFIPTM 2013, Malaga, Spain, June 3-7, 2013, pp. 1–16.
http://link.springer.com/chapter/10.1007%2F978-3-642-38323-6_1#.

[53] Thijs Laarhoven and Benne de Weger,
"Discrete Distributions in the Tardos Scheme, Revisited",
in: *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec'13, Montpellier, France, June 17-19, 2013)*, ACM, New York, 2013, pp. 13–17,
http://deweger.xs4all.nl/papers/[54]LdW-DiscrTardos[2013].pdf.

[54] Benne de Weger,
"A generalized Ramanujan-Nagell equation related to certain strongly regular graphs",
Integers 14 [2014], Article A35,
http://www.integers-ejcnt.org/vol14.html.

[55] Benne de Weger,
"Het $3n+1$-vermoeden",
Nieuw Archief voor Wiskunde **5/15** [2014], 40–50,
http://deweger.xs4all.nl/papers/[56]dW-Coll-NAW[2014].pdf.

[56] Thijs Laarhoven and Benne de Weger,
"Faster sieving for shortest lattice vectors using spherical locality-sensitive hashing",
Cryptology ePrint Archive, Report 2015/211,
http://eprint.iacr.org/2015/211,
in: K. Lauter and F. Rodríguez-Henríquez (eds.), *LatinCrypt 2015*, Lecture Notes in Computer Science Vol. 9230, Springer, Berlin, 2015, pp. 101–118.

[57] Aart Blokhuis, Andries Brouwer and Benne de Weger,
"Binomial collisions and near collisions",
Integers 17 [2017], Article A64,
http://www.integers-ejcnt.org/vol17.html.

[58] Emmanouil Doulgerakis, Thijs Laarhoven and Benne de Weger,
"Finding Closest Lattice Vectors Using Approximate Voronoi Cells",
in: J. Ding and R. Steinwandt (Eds.): *PQCrypto 2019*, Lecture Notes in Computer Science Vol. 11505, Springer, Berlin, 2019, pp. 3–22.

Software

Benne de Weger,
"MCR - Modulaire en Cryptografische Rekenmachine",
java application, 2009–2018 (versie 4: 2016, versie E (met elliptische krommen): 2018),
http://www.win.tue.nl/~bdeweger/MCR/.

Benne de Weger,
"BCC - BraboCoin Calculator",
java application, version 1.1, 2019,
https://www.win.tue.nl/~bdeweger/downloads/BCCv1.0.jar,
https://www.win.tue.nl/~bdeweger/downloads/BCCv1.0.exe.

Websites

Arjen Lenstra, Xiaoyun Wang, Benne de Weger,
"Colliding X.509 Certificates based on MD5-collisions",
http://www.win.tue.nl/~bdeweger/CollidingCertificates/,
March 2005.

Marc Stevens, Arjen Lenstra, Benne de Weger,
"HashClash",
http://www.win.tue.nl/hashclash/,
2006.

Marc Stevens, Arjen Lenstra, Benne de Weger,
"Colliding X.509 Certificates for Different Identities",
http://www.win.tue.nl/hashclash/TargetCollidingCertificates/,
October 2006.

Marc Stevens, Arjen Lenstra, Benne de Weger,
"Chosen-prefix collisions",
http://www.win.tue.nl/hashclash/ChosenPrefixCollisions/,
February 2007.

Marc Stevens, Arjen Lenstra, Benne de Weger,
"Predicting the winner of the 2008 US Presidential Elections using a Sony PlayStation 3",
http://www.win.tue.nl/hashclash/Nostradamus/,
November 2007.

Marc Stevens, Arjen Lenstra, Benne de Weger,
"Vulnerability of software integrity and code signing applications to chosen-prefix collisions for MD5",
http://www.win.tue.nl/hashclash/SoftIntCodeSign/,
November 2007.

Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger,
"MD5 considered harmful today - Creating a rogue CA certificate",
http://www.win.tue.nl/hashclash/rogue-ca/,
December 2008.
▷ Translated into Korean (http://www.securityproof.org/md5.pdf).
▷ Translated into Belorussian (http://www.movavi.com/opensource/rogue-ca-be).

Marc Stevens, website by Benne de Weger,
"A Single Block Chosen Prefix Collision for MD5",
http://www.win.tue.nl/hashclash/SingleBlock/,
June 2009.

Reports

Only those reports are mentioned that were not published otherwise.

C. Hoede, A.A. Jagers, H.J. Veldman and B.M.M. de Weger (eds.),
"Memorandum No. 1000",
Memorandum 1000, Faculty of Applied Mathematics, University of Twente, 1991.

B.M.M. de Weger,
"Thue equations related to the same unit equation",
Report 9475/B, Econometric Institute, Erasmus University Rotterdam, 1994.
http://deweger.xs4all.nl/papers/[1994]EcInst-9475B.pdf

Benjamin M.M. de Weger,
"Complete solution of a Thue inequality",
Report 9561/B, Econometric Institute, Erasmus University Rotterdam, 1995.
http://deweger.xs4all.nl/papers/[1995]EcInst-9561B.pdf

Engelbert Hubbers, Bart Jacobs, Berry Schoenmakers, Henk van Tilborg and Benne de Weger,
"Description and Analysis of the RIES Internet Voting System",
EiPSI report 0801, version 1.0, June 2008.
http://deweger.xs4all.nl/papers/[2008]RIES.pdf

Thijs Laarhoven, Joop van de Pol and Benne de Weger,
"Solving Hard Lattice Problems and the Security of Lattice-Based Cryptosystems",
Cryptology ePrint Archive, Report 2012/533,
http://eprint.iacr.org/2012/533,
http://deweger.xs4all.nl/papers/[51]LvdPdW-Kolkata[2012].pdf.

Maran van Heesch, Tanja Lange and Benne de Weger,
"Concrete security estimates for Ring-LWE based key exchange protocols", 2017.

Not 'officially' published notes

Benne de Weger,
"A new extreme abc-example",
August 1999,
http://deweger.xs4all.nl/oud/broberg.txt.

Benne de Weger,
"A newer extreme abc-example due to Tim Dokchitser",
August 2003,
http://deweger.xs4all.nl/oud/dokchitser.txt.

Benne de Weger,
"There are only a few Padovan squares in Padua",
November 2004,
http://www.win.tue.nl/~bdeweger/downloads/PadovanSquares.pdf

Benne de Weger,
"Dual Discrete Logarithms",
in: Liber Amicorum for Henk van Tilborg on the occasion of his 60th birthday, Eindhoven,
October 2007,
www.win.tue.nl/~bdeweger/downloads/Henk60.pdf.

Benne de Weger,
"Diophantische vergelijkingen in het kerstpakket",
December 2010,
http://www.win.tue.nl/~bdeweger/downloads/tue55.pdf.

Benne de Weger,
"Comments on Opfer's alleged proof of the $3n+1$ Conjecture",
version 0.2, June 2011,
http://www.win.tue.nl/~bdeweger/downloads/opfer-commentsv0.2.pdf.

Benne de Weger,
"Numerical data related to the Lagarias-Soundararajan xyz-conjecture",
version 1.3, May 2012,
http://www.win.tue.nl/~bdeweger/downloads/xyz_v1.3.pdf.
Accompanying file with data:
http://www.win.tue.nl/~bdeweger/downloads/xyz1737.txt.

Benne de Weger,
"Lagrange's Algorithm Strikes Again – How to write a prime as a sum of two squares",
version 1.0, July 2012,
http://www.win.tue.nl/~bdeweger/downloads/sumof2squares.pdf.

Educational articles

Benne de Weger,
"Securing e-business – Sicherung des e-Business",
Hoyer Journal, December 2000, p. 3.
http://deweger.xs4all.nl/papers/[2000]Hoyer.pdf

Benne de Weger,
"Hash-functies onder vuur",
Informatiebeveiliging (Platform voor Informatiebeveiliging) **2005**(4) [april 2005], 25–30.
http://deweger.xs4all.nl/papers/[2005]Informatiebeveiliging.pdf

Benne de Weger,
"Knoeiboelfuncties",
Supremum (Studievereniging Gewis, TU Eindhoven) **39**(4) [juni 2007], 36–37.
http://deweger.xs4all.nl/papers/[2007]Supremum.pdf

Benne de Weger,
"Zwakke sleutels bij het RSA-cryptosysteem, deel 1",
Euclides (Nederlandse Vereniging van Wiskundeleraren) **84**(7) [juni 2009], 256–260.
http://deweger.xs4all.nl/papers/[2009]Euclides1.pdf
▷ Erratum: *Euclides* (Nederlandse Vereniging van Wiskundeleraren) **84**(8) [juli 2009], 309.
http://deweger.xs4all.nl/papers/[2009]Euclides1a.pdf

Benne de Weger,
"Zwakke sleutels bij het RSA-cryptosysteem, deel 2",
Euclides (Nederlandse Vereniging van Wiskundeleraren) **84**(8) [juli 2009], 306–308.
http://deweger.xs4all.nl/papers/[2009]Euclides2.pdf

Benne de Weger,
"Hoe je het cryptosysteem RSA soms kunt kraken",
in: *Wiskunde: de uitdaging - Vakantiecursus 2010*, CWI Syllabus 60, Amsterdam, 2010.
http://www.win.tue.nl/~bdeweger/downloads/RSA-soms-kraken-tekst.pdf.

Benne de Weger,
"Het $3n+1$-vermoeden",
in: *Wiskunde in Wording - Vakantiecursus 2013*, Platform Wiskunde Nederland, Amsterdam, 2013.
http://www.win.tue.nl/~bdeweger/downloads/VC2013-BdW.pdf.

Benne de Weger,
"Praktikum",
in: *Dit is triviaal - Vakantiecursus 2015*, Platform Wiskunde Nederland, Amsterdam, 2015.
https://www.platformwiskunde.nl/wp-content/uploads/2016/10/VakantieCursus2015v1.21.pdf.

Benne de Weger,
"Cryptografie – de wetenschap van geheimen",
"De cryptografie achter Bitcoin",
"Cryptografische beveiliging op het internet",
in: *De wiskunde in je broekzak - Vakantiecursus 2018*, Platform Wiskunde Nederland, Amsterdam, 2018.
https://www.platformwiskunde.nl/wp-content/uploads/2018/09/VC-syllabus-2018_v1.1.pdf.

Educational Syllabi (editor)

De exacte benadering - Vakantiecursus 2012, Platform Wiskunde Nederland, Amsterdam, 2012.
https://www.platformwiskunde.nl/wp-content/uploads/2017/09/Syllabus_VC2012-def.pdf.

Wiskunde in wording - Vakantiecursus 2013, Platform Wiskunde Nederland, Amsterdam, 2013.
https://www.platformwiskunde.nl/wp-content/uploads/2016/10/VC2013syllabus-web.pdf.

Nieuwe tijden - Vakantiecursus 2014, Platform Wiskunde Nederland, Amsterdam, 2014.
https://www.platformwiskunde.nl/wp-content/uploads/2016/10/VakantieCursus2014v2.0.pdf.

Dit is triviaal - Vakantiecursus 2015, Platform Wiskunde Nederland, Amsterdam, 2015.
https://www.platformwiskunde.nl/wp-content/uploads/2016/10/VakantieCursus2015v1.21.pdf.

Netwerken - Vakantiecursus 2016, Platform Wiskunde Nederland, Amsterdam, 2016.
https://www.platformwiskunde.nl/wp-content/uploads/2016/10/Syllabus_VC2016_v1.1.pdf.

De computer in de wiskunde: breekijzer of oud schroot? - Vakantiecursus 2017, Platform Wiskunde Nederland, Amsterdam, 2017.
https://www.platformwiskunde.nl/wp-content/uploads/2017/09/Syllabus-VC-2017_v1.0.pdf.

De wiskunde in je broekzak - Vakantiecursus 2018, Platform Wiskunde Nederland, Amsterdam, 2018.
https://www.platformwiskunde.nl/wp-content/uploads/2018/09/VC-syllabus-2018_v1.1.pdf.

Course books

A.B. van Gool, H.M. Mulder, E.M. van de Vrie, B.M.M. de Weger en L.J.G.M. Wiegerinck,
Discrete Wiskunde,
4 delen, Open Universiteit, Heerlen, 1989.
▷ Heruitgegeven onder de titel *Combinatoriek, Grafen- en Getaltheorie* in 1996.

A.G. van Asch, R.J. Beerends, P.G.M. Bezembinder, J. van de Craats, J.S. Lodder, B.M.M. de Weger en G. Zwaneveld,
Continue Wiskunde 1,
5 delen, Open Universiteit, Heerlen, 1998.

Lecture Notes

P. le Grand, F. Twilt en B.M.M. de Weger,
"Analyse B voor WB, voor CT/INF, Analyse B (deel 1) voor TN",
Faculteit der Toegepaste Wiskunde, Universiteit Twente, 1992.

P. Jonker, P. le Grand, F. Twilt en B.M.M. de Weger,
"Analyse B voor EL",
Faculteit der Toegepaste Wiskunde, Universiteit Twente, 1992.

Benne de Weger,
"Mathematics for Information Security",
Faculteit Wiskunde en Informatica, Technische Universiteit Eindhoven, 2004.

Benne de Weger,
"Cryptographic Systems",
Faculteit Wiskunde en Informatica, Technische Universiteit Eindhoven, 2006.

Jan Draisma and Benne de Weger,
"Discrete Mathematics",
Faculteit Wiskunde en Informatica, Technische Universiteit Eindhoven, 2007.

Liber Amicorum

Bram van Asch, Anita Klooster, Berry Schoenmakers and Benne de Weger (eds.),
"KlabotsCrypt – Liber Amicorum voor Henk van Tilborg",
Faculteit Wiskunde en Informatica, Technische Universiteit Eindhoven, 2011.