NAME

Paul ZIMMERMANN, `www.loria.fr/~zimmerma`

Born November 13, 1964. French. Two children.

STUDIES

2001: "Habilitation à diriger des recherches" in comp. sc. (Univ. Nancy 1).
1988-1991: PhD thesis in computer science at École Polytechnique, (Palaiseau, France), entitled "Séries génératrices et analyse automatique d'algorithmes".
1987-1988: Master thesis in computer science at University Paris VII and "magistère" in mathematics and computer science at École Normale Supérieure.
1984-1987: engineer studies at École Polytechnique (Palaiseau, France).

EMPLOYMENTS

since April 1991: Research Fellow ("directeur de recherche" since October 1998) at Inria (Institut National de Recherche en Informatique et en Automatique), first in Rocquencourt, and from November 1992 in Nancy.
From October 1994 to September 1995: Visiting Position at University Paderborn (Germany) in the MuPAD group.

RESPONSIBILITIES

2013-2016: Scientific Director and Chair of the Projects Committee at Inria Nancy Grand-Est.
2006-2015: vice-head of the CACAO and CARAMEL teams at Inria Nancy Grand-Est.
1998-2006: head of the PolKA team, then of the SPACES-Nancy team at Inria Lorraine.
2001-2009: member of the program committee of the ARITH conference.
2006: member of the program and steering committee of the RNC conference, and program chair of RNC'7 (2006).

SOFTWARE

since 2005: main developers of CADO-NFS, a program to factor integer using the Number Field Sieve (NFS)
since 1999: MPFR (with V. Lefèvre, P. Pélissier, Ph. Théveny), a library for multiple-precision floating-point arithmetic with exact rounding (`www.mpfr.org`).
since 1998: GMP-ECM, a program for integer factorization using elliptic curves.
1994-1998: written many parts from the library of the MuPAD computer algebra system by the University of Paderborn (Germany). Implementation of many symbolic computation algorithms.
1992: Gfun (with Bruno Salvy), a Maple package for the manipulation of holonomic functions, distributed within Maple since version V.2.

AWARDS

Winner of the "Many Digits" Competition (Nijmegen, 2005)
2015 : best paper award at ACM CCS 2015 [89]

Articles

[1] Flajolet, P., Salvy, B., and Zimmermann, P. Automatic Average–case Analysis of Algorithms. *Theoretical Comput. Sci. 79*, 1 (1991), 37–109.

[2] Flajolet, P., Zimmermann, P., and Cutsem, B. V. A calculus for the random generation of labelled combinatorial structures. *Theoretical Comput. Sci. 132*, 1-2 (1994), 1–35.

[3] Louchard, G., Schott, R., Tolley, M., and Zimmermann, P. Random walks, heat equation and distributed algorithms. *Journal of Computational and Applied Mathematics 53* (1994), 243–274.

[4] Rivin, I., Vardi, I., and Zimmermann, P. The n-Queens Problem. *American Mathematical Monthly 101*, 7 (1994), 629–639.

[5] Salvy, B., and Zimmermann, P. Gfun: A Maple package for the manipulation of generating and holonomic functions in one variable. *ACM Trans. Math. Softw. 20*, 2 (1994), 163–177.

[6] Zimmermann, P. Gaïa: a package for the random generation of combinatorial structures. *MapleTech 1*, 1 (1994), 38–46.

[7] Zimmermann, P. Function composition and automatic average case analysis. *Discrete Mathematics 139* (1995), 443–453.

[8] Zimmermann, P. New features in MuPAD 1.2.2. *mathPAD 5*, 1 (1995), 27–38.

[9] Zimmermann, P. Wester's test suite in MuPAD 1.2.2. *Computer Algebra Nederland Nieuwsbrief*, 14 (1995), 53–64.

[10] Zimmermann, P. Wester's test suite in MuPAD 1.3. *SAC Newsletter*, 1 (1996).

[11] Zimmermann, P. Calcul formel : l'embarras du choix. *Gazette des Mathématiciens de la Société Mathématique de France 73* (1997), 39–43.

[12] Bertault, F., Ramaré, O., and Zimmermann, P. On sums of seven cubes. *Mathematics of Computation 68*, 227 (1999), 1303–1310.

[13] Denise, A., and Zimmermann, P. Uniform random generation of decomposable structures using floating-point arithmetic. *Theoretical Comput. Sci. 218*, 2 (1999), 219–232.

[14] Zimmermann, P. Arithmétique en précision arbitraire. *Réseaux et Systèmes Répartis, Calculateurs Parallèles 13*, 4-5 (2001), 357–386.

[15] Benito, M., Creyaufmüller, W., Varona, J. L., and Zimmermann, P. Aliquot sequence 3630 ends after reaching 100 digits. *Experimental Mathematics 11*, 2 (2002), 201–206.

[16] Bertot, Y., Magaud, N., and Zimmermann, P. A proof of GMP square root. *Journal of Automated Reasoning 29* (2002), 225–252. Special Issue on Automating and Mechanising Mathematics: In honour of N.G. de Bruijn.

[17] Dubner, H., Forbes, T., Lygeros, N., Mizony, M., Nelson, H., and Zimmermann, P. Ten consecutive primes in arithmetic progression. *Mathematics of Computation 71*, 239 (2002), 1323–1328.

[18] Brent, R. P., Larvala, S., and Zimmermann, P. A fast algorithm for testing reducibility of trinomials mod 2 and some new primitive trinomials of degree 3021377. *Mathematics of Computation 72*, 243 (2003), 1443–1452.

[19] Hanrot, G., Rivat, J., Tenenbaum, G., and Zimmermann, P. Density results on floating-point invertible numbers. *Theoretical Comput. Sci. 291*, 2 (2003), 135–141.

[20] Zimmermann, P. $10^{2098959}$. *Gazette du CINES*, 14 (2003).

[21] Defour, D., Hanrot, G., Lefèvre, V., Muller, J.-M., Revol, N., and Zimmermann, P. Proposal for a standardization of mathematical function implementation in floating-point arithmetic. *Numerical Algorithms 37*, 1-4 (2004), 367–375.

[22] Hanrot, G., Quercia, M., and Zimmermann, P. The middle product algorithm, I. Speeding up the division and square root of power series. *AAECC 14*, 6 (2004), 415–438.

[23] Hanrot, G., and Zimmermann, P. A long note on Mulders' short product. *Journal of Symbolic Computation 37* (2004), 391–401.

[24] Rouillier, F., and Zimmermann, P. Efficient isolation of a polynomial real roots. *Journal of Computational and Applied Mathematics 162*, 1 (2004), 33–50.

[25] Brent, R. P., Larvala, S., and Zimmermann, P. A primitive trinomial of degree 6972593. *Mathematics of Computation 74*, 250 (2005), 1001–1002.

[26] Gerard, Y., Debled-Rennesson, I., and Zimmermann, P. An elementary digital plane recognition algorithm. *Discrete Applied Mathematics 151*, 1–3 (2005), 169–183.

[27] Stehlé, D., Lefèvre, V., and Zimmermann, P. Searching worst cases of a one-variable function using lattice reduction. *IEEE Transactions on Computers 54*, 3 (2005), 340–346.

[28] Brent, R., Percival, C., and Zimmermann, P. Errors bounds on complex floating-point multiplication. *Mathematics of Computation 76*, 259 (2007), 1469–1481.

[29] Fousse, L., Hanrot, G., Lefèvre, V., Pélissier, P., and Zimmermann, P. MPFR: A multiple-precision binary floating-point library with correct rounding. *ACM Trans. Math. Softw. 33*, 2 (2007), article 13.

[30] Brent, R. P., and Zimmermann, P. A multi-level blocking distinct degree factorization algorithm. *Contemporary Mathematics 461* (2008), 47–58.

[31] Deléglise, M., Nicolas, J.-L., and Zimmermann, P. Landau's function for one million billions. *Journal de Théorie des Nombres de Bordeaux 20*, 3 (2008), 625–671.

[32] Brent, R. P., and Zimmermann, P. Ten new primitive binary trinomials. *Mathematics of Computation 78*, 266 (2009), 1197–1199.

[33] Rump, S., Zimmermann, P., Boldo, S., and Melquiond, G. Computing predecessor and successor in rounding to nearest. *BIT Numerical Mathematics 49*, 2 (2009), 419–431.

[34] Ghazi, K. R., Lefèvre, V., Théveny, P., and Zimmermann, P. Why and how to use arbitrary precision. *Computing in Science and Engineering 12*, 3 (2010), 62–65.

[35] Brent, R. P., and Zimmermann, P. The great trinomial hunt. *Notices of the AMS 58*, 2 (2011), 233–239. Invited paper, see also `arXiv:1005.1967`.

[36] Prest, T., and Zimmermann, P. Non-linear polynomial selection for the number field sieve. *Journal of Symbolic Computation 47*, 4 (2012), 401–409.

[37] Melquiond, G., Nowak, W. G., and Zimmermann, P. Numerical approximation of the Masser-Gramain constant to four decimal digits: $\delta = 1.819...$. *Mathematics of Computation 82*, 282 (2013), 1235–1246.

[38] Bouvier, C., and Zimmermann, P. Division-Free Binary-to-Decimal Conversion. *IEEE Transactions on Computers 63*, 8 (Aug. 2014), 1895–1901.

[39] Bai, S., Bouvier, C., Kruppa, A., and Zimmermann, P. Better polynomials for GNFS. *Mathematics of Computation 85* (2016), 861–873.

Theses

[40] Zimmermann, P. *Séries génératrices et analyse automatique d'algorithmes.* Thèse de doctorat, École Polytechnique, Palaiseau, 1991.

[41] Zimmermann, P. *De l'algorithmique à l'arithmétique via le calcul formel.* Habilitation à diriger des recherches, Université Henri Poincaré Nancy 1, 2001.

Books

[42] Gomez, C., Salvy, B., and Zimmermann, P. *Calcul formel : mode d'emploi. Exemples en Maple.* Masson, 1995.

[43] Fuchssteiner, B., Drescher, K., Kemper, A., Kluge, O., Morisse, K., Naundorf, H., Oevel, G., Postel, F., Schulze, T., Siek, G., Sorgatz, A., Wiwianka, W., and Zimmermann, P. *MuPAD User's Manual.* Wiley Ltd., 1996.

[44] Brent, R. P., and Zimmermann, P. *Modern Computer Arithmetic.* No. 18 in Cambridge Monographs on Applied and Computational Mathematics. Cambridge University Press, 2010. Electronic version freely available at `http://www.loria.fr/~zimmerma/mca/pub226.html`.

[45] Casamayou, A., Cohen, N., Connan, G., Dumont, T., Fousse, L., Maltey, F., Meulien, M., Mezzarobba, M., Pernet, C., Thiéry, N. M., and Zimmermann, P. *Calcul mathématique avec Sage.* CreateSpace, 2013. Electronic version available under Creative Commons license, `http://sagebook.gforge.inria.fr/`.

Proceedings

[46] Müller, N., Escardo, M., and Zimmermann, P., Eds. *Special issue on practical development of exact real number computation* (2005). Journal of Logic and Algebraic Programming, vol. 64, nb. 1, 154 pages.

[47] Hanrot, G., and Zimmermann, P., Eds. *Proceedings of the 7th Conference on Real Numbers and Computers (RNC'7)* (Nancy, France, 2006), Institut National Polytechnique de Lorraine. 151 pages.

In Books

[48] Zimmermann, P. *Encyclopedia of Cryptography and Security.* Springer, 2005, ch. The Elliptic Curve Method, pp. 190–191. Van Tilborg, Henk C.A. (Ed.).

[49] Zimmermann, P. *Encyclopédie de l'informatique et des systèmes d'information.* Vuibert, 2006, ch. Techniques algorithmiques et méthodes de programmation, pp. 929–935.

In Collection

[50] Zimmermann, P. Calcul formel : ce qu'il y a dans la boîte. In *Journées X-UPS 97*, N. Berline and C. Sabbah, Eds. École Polytechnique, Palaiseau, France, 1997, pp. 47–62.

[51] Postel, F., and Zimmermann, P. Solving ordinary differential equations. In *Computer Algebra Systems: A Practical Guide*, M. Wester, Ed. John Wiley & Sons Ltd, 1999, pp. 191–209.

Conference Communications

[52] Flajolet, P., Salvy, B., and Zimmermann, P. Lambda–Upsilon–Omega: An Assistant Algorithms Analyzer. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (1989), T. Mora, Ed., vol. 357 of *Lecture Notes in Computer Science*, pp. 201–212.

[53] Albert, L., Casas, R., Fages, F., Torrecillas, A., and Zimmermann, P. Average case analysis of unification algorithms. In *Proceedings of STACS'91* (1991), C. Choffrut and M. Jantzen, Eds., vol. 480 of *Lecture Notes in Computer Science*, pp. 196–213.

[54] Zimmermann, P., and Zimmermann, W. The Automatic Complexity Analysis of Divide-and-Conquer Algorithms. In *Computer and Information Sciences VI* (1991), Elsevier, pp. 395–404.

[55] Zimmermann, P. Function composition and automatic average case analysis. In *Proceedings of the 4th Colloquium Séries formelles et combinatoire algébrique* (1992), P. Leroux and C. Reutenauer, Eds., vol. 11 of *Publications du LACIM, Université du Québec à Montréal*, pp. 477–486.

[56] Flajolet, P., Zimmermann, P., and Cutsem, B. V. A calculus of random generation. In *Proceedings of the First European Symposium on Algorithms (ESA'93)* (Bad Honnef, 1993), T. Lengauer, Ed., no. 726 in Lecture Notes in Computer Science, pp. 169–180.

[57] Drescher, K., and Zimmermann, P. Gröbner bases in MuPAD: state and future. In *Proceedings of the PoSSo workshop on software, Paris* (1995), pp. 177–182.

[58] Zimmermann, P. Uniform random generation for the powerset construction. In *Proceedings of the 7th conference on Formal Power Series and Algebraic Combinatorics* (Marne-la-Vallée, 1995), B. Leclerc and J.-Y. Thibon, Eds., pp. 589–600.

[59] Postel, F., and Zimmermann, P. A review of the ODE solvers of Axiom, Derive, Maple, Mathematica, Macsyma, MuPAD and Reduce. In *Proceedings of the 5th RHINE workshop on computer algebra* (Saint-Louis, France, 1996), A. Carrière and L. R. Oudin, Eds., pp. 2.1–2.10.

[60] Denise, A., Dutour, I., and Zimmermann, P. Cs: a MuPAD package for counting and randomly generating combinatorial structures. In *Proceedings of FPSAC'98* (1998), pp. 195–204. Sofware Demonstration.

[61] Lygeros, N., Mizony, M., and Zimmermann, P. Sur la division euclidienne d'un nombre premier par son rang. In *Journée de Mathématiques Effectives en l'honneur des 65 ans de René Ouzilou. Pré-Publication numéro 7 du Département de Mathématiques de l'Université Jean Monnet* (1998).

[62] Bertault, F., and Zimmermann, P. Unranking of unlabelled decomposable structures. In *Proceedings of Ordal'99, Montpellier* (1999).

[63] Cavallar, S., Dodson, B., Lenstra, A., Leyland, P., Lioen, W., Montgomery, P., Murphy, B., te Riele, H., and Zimmermann, P. Factorization of RSA-140 using the number field sieve. In *Advances in Cryptology, Asiacrypt'99* (Berlin, 1999), L. K. Yan, E. Okamoto, and X. Chaoping, Eds., vol. 1716 of *Lecture Notes in Computer Science*, Springer, pp. 195–207.

[64] Zimmermann, P. GMP-ECM: yet another implementation of the Elliptic Curve Method (or how to find a 40-digit prime factor within $2 \cdot 10^{11}$ modular multiplications). In *workshop* Computational Number Theory*, FoCM'99, Oxford* (1999). Invited talk.

[65] Abbott, J., Shoup, V., and Zimmermann, P. Factorization in Z[x]: the searching phase. In *Proceedings of ISSAC'2000* (2000), C. Traverso, Ed., ACM Press, pp. 1–7.

[66] Cavallar, S., Dodson, B., Lenstra, A. K., Lioen, W., Montgomery, P. L., Murphy, B., te Riele, H., Aardal, K., Gilchrist, J., Guillerm, G., Leyland, P., Marchand, J., Morain, F., Muffett, A., Putnam, C., Putnam, C., and Zimmermann, P. Factorization of a 512–bit RSA modulus. In *Proceedings of Eurocrypt'2000* (Bruges, Belgium, 2000), B. Preneel, Ed., vol. 1807 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 1–18.

[67] Zimmermann, P. Symbolic computation: Recent progress and new frontiers. In *Proceedings of SCAN'02* (2002). Invited conference.

[68] Brent, R., and Zimmermann, P. Algorithms for finding almost irreducible and almost primitive trinomials. In *Primes and Misdemeanours: Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams* (Banff, Canada, 2003), A. van der Poorten and A. Stein, Eds., The Fields Institute, Toronto, pp. 91–102. Invited paper. Published by the AMS, 2004.

[69] Brent, R., and Zimmermann, P. Random number generators with period divisible by a Mersenne prime. In *Proceedings of Computational Science and its Applications (ICCSA)* (2003), no. 2667 in Lecture Notes in Computer Science, Springer-Verlag, pp. 1–10. Invited paper.

[70] Fousse, L., and Zimmermann, P. Accurate summation: Towards a simpler and formal proof. In *Proceedings of the RNC'5 conference (Real Numbers and Computers)* (2003), pp. 97–108.

[71] Stehlé, D., Lefèvre, V., and Zimmermann, P. Worst cases and lattice reduction. In *Proceedings of the 16th IEEE Symposium on Computer Arithmetic* (2003), J.-C. Bajard and M. Schulte, Eds., IEEE Computer Society, pp. 142–147.

[72] Stehlé, D., and Zimmermann, P. A binary recursive gcd algorithm. In *Proceedings of the 6th International Symposium on Algorithmic Number Theory (ANTS VI)* (Burlington, USA, 2004), D. A. Buell, Ed., vol. 3076 of *Lecture Notes in Computer Science*, pp. 411–425.

[73] Stehlé, D., and Zimmermann, P. Gal's accurate tables method revisited. In *Proceedings of the 17th IEEE Symposium on Computer Arithmetic (ARITH'17)* (2005), P. Montuschi and E. Schwarz, Eds., IEEE Computer Society, pp. 257–264.

[74] Zimmermann, P. Can we trust floating-point numbers? In *"Grand Challenges of Informatics", An Academia Europaea Charles Simonyi John von Neumann Computer Society International Symposium* (Budapest, Hungary, 2006). Invited conference.

[75] Zimmermann, P., and Dodson, B. 20 years of ECM. In *Proceedings of the 7th Algorithmic Number Theory Symposium (ANTS VII)* (Berlin Heidelberg, 2006), F. Hess, S. Pauli, and M. Pohst, Eds., vol. 4076 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 525–542.

[76] Brent, R. P., and Zimmermann, P. A multi-level blocking distinct degree factorization algorithm. In *Proceedings of the 8th International Conference on Finite Fields and Applications (Fq8)* (Melbourne, Australia, 2007). Extended abstract.

[77] Cheng, H., Hanrot, G., Thomé, E., Zima, E., and Zimmermann, P. Time- and space-efficient evaluation of some hypergeometric constants. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, ISSAC'2007* (Waterloo, Ontario, Canada, 2007), C. W. Brown, Ed., ACM, pp. 85–91.

[78] Gaudry, P., Kruppa, A., and Zimmermann, P. A GMP-based implementation of Schönhage-Strassen's large integer multiplication algorithm. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, ISSAC'2007* (Waterloo, Ontario, Canada, 2007), C. W. Brown, Ed., pp. 167–174.

[79] Hanrot, G., Lefèvre, V., Stehlé, D., and Zimmermann, P. Worst cases of a periodic function for large arguments. In *Proceedings of the 18th IEEE Symposium on Computer Arithmetic (ARITH'18)* (Montpellier, France, 2007), P. Kornerup and J.-M. Muller, Eds., IEEE Computer Society Press, Los Alamitos, CA, pp. 133–140.

[80] Brent, R., Gaudry, P., Thomé, E., and Zimmermann, P. Faster multiplication in GF(2)[x]. In *Proceedings of the 8th International Symposium on Algorithmic Number Theory (ANTS VIII)* (2008), A. J. van der Poorten and A. Stein, Eds., vol. 5011 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 153–166.

[81] Lefèvre, V., Stehlé, D., and Zimmermann, P. Worst cases for the exponential function in the IEEE 754r decimal64 format. In *Reliable Implementation of Real Number Algorithms: Theory and Practice* (2008), P. Hertling, C. M. Hoffmann, W. Luther, and N. Revol, Eds., no. 5045 in Lecture Notes in Computer Science, pp. 114–126.

[82] Brent, R. P., and Zimmermann, P. An $O(M(n)\log n)$ algorithm for the Jacobi symbol. In *Proceedings of the 9th Algorithmic Number Theory Symposium (ANTS-IX)* (Nancy, France, 2010), G. Hanrot, F. Morain, and E. Thomé, Eds., vol. 6197 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 83–95.

[83] Kleinjung, T., Aoki, K., Franke, J., Lenstra, A. K., Thomé, E., Bos, J. W., Gaudry, P., Kruppa, A., Montgomery, P. L., Osvik, D. A., te Riele, H., Timofeev, A., and Zimmermann, P. Factorization of a 768-bit RSA modulus. In *Advances in Cryptology - CRYPTO 2010* (Santa Barbara, USA, 2010), T. Rabin, Ed., vol. 6223 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 333–350.

[84] Zimmermann, P. Reliable computing with GNU MPFR. In *Proceedings of the third International Congress on Mathematical Software (ICMS 2010)* (Kobe, Japan, 2010), K. Fukuda, J. van der Hoeven, M. Joswig, and N. Takayama, Eds., vol. 6327 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 42–45. Invited talk.

[85] Cortier, V., Detrey, J., Gaudry, P., Sur, F., Thomé, E., Turuani, M., and Zimmermann, P. Ballot stuffing in a postal voting system. In *Revote 2011 - International Workshop on Requirements Engineering for Electronic Voting Systems* (Trento, Italy, 2011), IEEE, pp. 27 – 36.

[86] Harvey, D., and Zimmermann, P. Short Division of Long Integers. In *20th IEEE Symposium on Computer Arithmetic (ARITH-20)* (Tuebingen, Germany, July 2011), E. Antelo, D. Hough, and P. Ienne, Eds., IEEE, pp. 7–14.

[87] Barbulescu, R., Detrey, J., Estibals, N., and Zimmermann, P. Finding Optimal Formulae for Bilinear Maps. In *International Workshop of the Arithmetics of Finite Fields* (Bochum, Germany, July 2012), F. Özbudak and F. Rodríguez-Henríquez, Eds., vol. 7369 of *Lecture Notes in Computer Science*, Ruhr Universitat Bochum.

[88] Barbulescu, R., Bouvier, C., Detrey, J., Gaudry, P., Jeljeli, H., Thomé, E., Videau, M., and Zimmermann, P. Discrete logarithm in GF(2^{809}) with FFS. In *PKC 2014 - International Conference on Practice and Theory of Public-Key Cryptography* (Buenos Aires, Argentina, 2014), H. Krawczyk, Ed., LNCS, Springer.

[89] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomé, E., Valenta, L., Vandersloot, B., Wustrow, E., Zanella-Béguelin, S., and Zimmermann, P. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. In *ACM CCS 2015* (Denver, Colorado, United States, Oct. 2015), p. 14.

[90] Zimmermann, P. Multiple precision: from MP to MPFR. In *4th Number Theory Down Under conference, Newcastle, Australia* (2016). Invited talk, `https://members.loria.fr/PZimmermann/talks.html`.

Research Reports

[91] Zimmermann, P. Alas : un système d'analyse algébrique. Rapport de DEA, Université de Paris VII, 1988. 120 pages. Disponible aussi en rapport de recherche INRIA (numéro 968).

[92] Flajolet, P., Salvy, B., and Zimmermann, P. Lambda–Upsilon–Omega: The 1989 Cookbook. Rapport de recherche 1073, Institut National de Recherche en Informatique et en Automatique, 1989. 116 pages.

[93] Hervé, J.-C., Morain, F., Salesin, D., Serpette, B.-P., Vuillemin, J., and Zimmermann, P. BigNum : un module portable et efficace pour une arithmétique à précision arbitraire. Rapport de recherche 1016, Institut National de Recherche en Informatique et en Automatique, 1989. 23 pages.

[94] Flajolet, P., and Zimmerman, P. Algorithms seminar, 1991–1992. Research Report 1779, Institut National de Recherche en Informatique et en Automatique, 1992. 192 pages.

[95] Zimmermann, P. Analysis of functions with a finite number of return values. Research Report 1625, Institut National de Recherche en Informatique et en Automatique, 1992.

[96] Zimmermann, P. Epelle : un logiciel de détection de fautes d'orthographe. Rapport de Recherche 2030, Institut National de Recherche en Informatique et en Automatique, 1993.

[97] Heckler, C., Metzner, T., and Zimmermann, P. Progress report on parallelism in MuPAD. Research Report 3154, Institut National de Recherche en Informatique et en Automatique, 1997. 14 pages.

[98] Zimmermann, P. Cinq algorithmes de calcul symbolique. Rapport Technique 206, Institut National de Recherche en Informatique et en Automatique, 1997.

[99] Dutour, I., Habsieger, L., and Zimmermann, P. Estimations asymptotiques du nombre de chemins Nord-Est de pente fixée et de largeur bornée. Research Report 3585, Institut National de Recherche en Informatique et en Automatique, 1998.

[100] Zimmermann, P. Karatsuba square root. Research Report 3805, INRIA, 1999.

[101] Belabas, K., Hanrot, G., and Zimmermann, P. Tuning and generalizing Van Hoeij's algorithm. Research Report 4124, Institut National de Recherche en Informatique et en Automatique, 2001. 13 pages.

[102] Lefèvre, V., and Zimmermann, P. Arithmétique flottante. Rapport de recherche 5105, Institut National de Recherche en Informatique et en Automatique, 2004. 60 pages.

Other publications

[103] Brent, R. P., Orrick, W. H., Osborn, J. H., and Zimmermann, P. Maximal determinants and saturated D-optimal designs of orders 19 and 37. Available from `https://members.loria.fr/PZimmermann/papers/rpb244.pdf`.

[104] Zimmermann, P. Commercial vs free computer algebra systems. Lecture to the 2nd IMACS conference in Linz, 1996.

[105] Zimmermann, P., Bernardin, L., and Monagan, M. Polynomial factorization challenges, 1996. Poster at ISSAC'96.

[106] Zimmermann, P. A proof of GMP fast division and square root implementations. http://www.loria.fr/~zimmerma/papers/proof-div-sqrt.ps.gz, 2000. 14 pages.

[107] Castiel, A., Lefèvre, V., and Zimmermann, P. Le «dilemme du fabricant de tables» ou comment calculer juste, 2004. Article de vulgarisation, http://interstices.info/display.jsp?id=c_5936.

[108] Hanrot, G., and Zimmermann, P. Newton iteration revisited. http://www.loria.fr/~zimmerma/papers/fastnewton.ps.gz, 2004. 2 pages.

[109] Zimmermann, P. Modular arithmetic. 8th Central European Conference on Cryptography, 2008. Invited talk, http://www.loria.fr/~zimmerma/talks.

[110] Bai, S., Thomé, E., and Zimmermann, P. Factorisation of RSA-704 with CADO-NFS, 2012. Preprint.

[111] Bai, S., Gaudry, P., Kruppa, A., Thomé, E., and Zimmermann, P. Factorisation of RSA-220 with CADO-NFS. https://hal.inria.fr/hal-01315738, 2016. 3 pages.