z

CURRICULUM VITAE

IGOR E. SHPARLINSKI

Address.
Department of Pure Mathematics
University of New South Wales
NSW 2109, Australia
Ph. [61-(0)2] 9385 5281
E-mail: igor.shparlinski@unsw.edu.au
Home page: http://web.maths.unsw.edu.au/~igorshparlinski

Personal.
Date of birth: January 13, 1956
Place of birth: Kiev, Ukraine
Nationality: Australian

Education.

- M.S. in Mathematics, Moscow State Pedagogical Institute, Faculty of Mathematics, 1977;
- Ph.D. in Mathematics, Moscow State Pedagogical Institute, Faculty of Mathematics, 1980.

Awards.

- Discovery Outstanding Research Award, 2014.
- Jean Morlet Chair, CIRM, Luminy, 2014.
- Distinguished Professor, Macquarie University, 2010.
- Telecom Chair in Security of Telecommunications, ENS-Paris, 2010.
- Fellow of the Australian Academy of Science, 2006.
- Australian Professorial Fellow, 2004.
- Fellow of the Australian Mathematical Society, 2000.
- Richard Miller Visiting Scholar in Mathematics (University of Missouri), 1999.
- Medal of the Australian Mathematical Society, 1996.
- Humboldt Professorship, DFG, Germany, 1996.

Grants.

- Large/Discovery Grants of the Australian Research Council, 1997-2019max
- Gold Star Grant of UNSW, 2016
- Theeman Travel Grant of the Israel Academy of Science, 1999, 2007
- Grant of the Royal Society, UK, 2003
- Grant of the Spanish Ministry of Education, 2003
- Small Grants of the Australian Research Council, 1995–2001
- Special Travel Grant of the Australian Academy of Science, 1998, 2002
- Macquarie University Research Grants, 1992–2002

Employment.

2013– Professor (Faculty of Science, UNSW);

2005–2013 Professor (Faculty of Science, Macquarie University);

2001–2004 Associate Professor (Division of Information and Communication Sciences, Macquarie University);

1996–2000 Senior Lecturer (Division of Information and Communication Sciences, Macquarie University);

1992–1995 Lecturer (School of Mathematics, Physics, Computing and Electronics, Macquarie University);

1987–1992 Senior Lecturer (Dept. of Computer Science, Moscow Institute of Radioengineering, Electronics and Automatics)

1980–1987 Lecturer (Dept. of Math., Moscow State Pedagogical Institute);

1990–1992 Senior Research Fellow (International Centre for Scientific and Technical Information);

1977–1990 Senior Research Fellow (Laboratory of Computer Science, Institute of Radioengineering and Electronics of the Academy of Science of the USSR).

Research Activities.
I am mainly interested in number theory, including its classical and more applied aspects. In many cases my results are still the best known. The main areas of my expertise where I believe I have achieved most important results and solved several long standing open questions are:

- Exponential sums, in particular I proved new bounds on Gaussian sums that improve the classical bound which I also used to established Stechkin's conjecture about these sums.
- Arithmetic problems in finite fields. I obtained new results about the distribution of primitive and irreducible polynomials in finite fields. In particular, I proved the existence of primitive and irreducible polynomials with very small coefficients or which are quite sparse.
- Distribution of rational points on curves and more general varieties over finite fields: I am especially interested in results about the distribution of points in small boxes that go beyond the capabilities of algebraic geometry methods. In particular, I obtained several results that break the square-root barrier imposed by the Weil and Deligne bounds and their extensions. An illustrative result is my solution of the Erdős–Graham problem about reciprocals of small integers. These results are often based on a combinbation of methods of arithmetic combinatorics (such as extensions of the sum-product theorem) and effective algebraic geometry (such as the theory of heights and arithmetic Hilbert's Nullstellensatz).
- Arithmetic properties of dynamical systems, including recurrence sequences. Such questions are notoriously hard, for example even for the simplest binary recurrence sequences such as $2^n + 1$ and $2^n - 1$ we still do not know whether they contain infinitely many primes.
- Using analytic number theory to derive rigorous proofs of various heuristic assumptions and conjectures in cryptography and computer science in the above area. Examples include:
  - New fast rigorously proved algorithms for deterministic polynomial factorization: based on bounds of double character sums of interval and so-called h-spaced sets;
  - establishing so-called *bit security* of the Diffie-Hellman key and also devising rigorous *attacks* on DSA, Nyberg-Rueppel and similar signature schemes: based on a combination of lattice basis algorithms, such as LLL, bounds various exponential sums, single and double, and tools from the theory of uniformity of distribution.
  - study various properties of graphs, such as iso-spectrality of circulant graphs: based on using equations in roots of unity.

Teaching Activities.
Since my appointment in October 1992 as Lecturer in the Computing at Macquarie University I have participated in a variety of teaching activities at all levels. I have taught the following courses

- Algorithm Theory and Design;
- Algorithms and Data Structures;
- Cryptography;
- Optimisation;
- Computer Graphics;

- Numerical Analysis;
- Algebraic and Symbolic Computation;
- Computing and Information Systems;
- Foundations of Computer Science;
- Introduction to **C**;
- Computer Architecture;
- Computational Science

I supervise 13 Honours, Masters and PhD students whose studies are successfully progressing (some of them have already published several papers related to their project).

Publications.
Papers in J. Reine Angew. Math., Compositio Math., Intern. Math. Research Notices, Math. Research Letter, Trans. Amer. Math. Soc., Israel J. Math., SIAM J. Math., Found. of Comp. Math., Math. Comp.
I also published several books and edited conference proceedings.

Editor Boards. :

- J. of the Australian Mathematical Society (Aust. Math. Soc.);
- Finite Fields and their Applications (Elsevier);
- Designs, Codes and Cryptography (Springer);
- SIAM J. Computing (SIAM);
- Mathematics of Computation (Amer. Math. Soc.);
- J. Mathematical Cryptology (Walter de Gruyter);
- Revista Matematica Complutense (Madrid);
- Contributions to Discrete Mathematics (Univ. of Calgary).

Organising and Chairing Conferences, Workshops, Competitions:

- Workshop on Algebraic, Number Theoretic and Graph Theoretic Aspects of Dynamical Systems, Sydney, Australia, 2-6 February, 2015;
- Thematic month "Arithmetics" at CIRM-Luminy, 2 February – March, 2014;
- RICAM Workshop on Emerging Applications of Finite Fields, Linz, Austria, 9-13 December, 2013;
- BIT-MPIM Workshop on Number Theory and Cryptography, Max Planck Institute for Mathematics, Bonn, 20-21 November, 2013;
- Banff Workshop on The Art of Iterating Rational Functions over Finite Fields, Banff, Canada, 5-10 May, 2013;
- International Workshop on Dynamical Systems and Number Theory in Memory of Alf van der Poorten, Macquarie Univ., Sydney, Australia, 19-20 March, 2012;
- International Number Theory Conference in Memory of Alf van der Poorten, Univ. of Newcastle, Newcastle, Australia, 12-16 March, 2012;
- AMS-SIAM Special Session on Mathematics of Computation: Algebra and Number Theory, Boston, MA, 4-8 January, 2012;
- AMS-SIAM Special Session on Mathematics of Computation: Algebra and Number Theory, New Orleans, LA, 6-9 January, 2011;
- Workshop on Dynamical Systems and Number Theory, Macquarie Univ., Sydney, Australia, 1 December, 2010;
- Workshop on Dynamical Systems and Uniform Distribution, Technical Univ. Graz, 28-29 January, 2010;
- Fields Institute Semester Program on Cryptography, Toronto, Canada, 2009;
- The 8th Algorithmic Number Theory Symposium, ANTS-8, Banff, Canada, 2008;
- Banff Workshop on Number Theory Inspired by Cryptography, Banff, Canada, 2005;
- Oberwolfach Meeting on Finite Fields and their Applications, Oberwolfach, Germany, 2004;

- The 14th Symposium Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Melbourne, 2001;
- Oberwolfach Meeting on Finite Fields and their Applications, Oberwolfach, Germany, 2001;
- The Workshop on Computational Number Theory and Cryptography, Singapore, 1999;
- The Conference on Finite Fields and their Applications, Oberwolfach, Germany, 1997;
- The joint Workshop of Mathematical and Computer Departments (Principal Organiser), Macquarie University, Australia, 1995;
- The 2nd Conference on Computational Algebra and Number Theory, Macquarie Univ., Australia, 1994–1995;
- The Student Competition "Information, Algorithms and Data Structures" (Principal Organiser), Macquarie University, Australia, 1995;
- The Conference on Number Theoretic and Algebraic Methods in Computer Science, Moscow, Russia, 1992–1994.

Program Committees.

- The 11th Algorithmic Number Theory Symposium, ANTS-IX, GyeongJu, South, Korea 2014;
- Public Key Cryptography, PKC'12, 2012;
- Eurorypt'12, Cambridge, UK, 2012;
- The 22nd International Symposium on Algorithms and Computation, ISAAC2011, Yokohama, Japan, 2011;
- The 27th Journees Arithmetiques, JA2011, Vilnius, Lithuania, 2011;
- Public Key Cryptography, PKC'10, Paris, France, 2010;
- The 9th Algorithmic Number Theory Symposium, ANTS-IX, Nancy, France, 2010;
- The 2nd International Conference on Symbolic Computation and Cryptography, SCC'10, Egham, UK, 2010;
- The 5th Latin American Theoretical Informatics Conf., LATIN'10, Oaxaca, México, 2010;
- Finite Fields and Applications, $\mathbb{F}_{q^9}$, Dublin, Ireland, 2009;
- Crypto'09, Santa Barbara, CA, 2009.
- Public Key Cryptography, PKC'09, Irvine, California, 2009.
- International Conference on Pairing-based Cryptography, Pairing'08, London, UK, 2008.
- International Symposium on Symbolic and Algebraic Computation, ISSAC2008, Hagenberg, Austria, 2008.
- Finite Fields and Applications, $\mathbb{F}_{q^8}$, Melbourne, Australia, 2007;
- International Conference on Pairing-based Cryptography, Pairing'07, Tokyo, Japan, 2007.
- International Workshop on the Arithmetic of Finite Fields, WAIFI'07, Madrid, Spain, 2007
- Symposium on Algebraic Geometry and its Applications, SAGA 2007, Tahiti, French Polynesia, 2007;
- Public Key Cryptography, PKC'07, Beijing, China, 2007;
- Eurocrypt'05, Aarhus, Denmark, 2005;
- The 9th Australasian Conference on Information Security and Privacy (ACISP04), July 13-15, Sydney, Australia, 2004;
- Eurocrypt'04, Interlaken, Switzerland, 2004;
- The 6th Algorithmic Number Theory Symposium, ANTS-VI, Annapolis, MD, US, 2004;
- The 8th Intern. Computing and Combinatorics Conf., COCOON'02, Singapore, 2002;
- The 5th Latin American Theoretical Informatics Conf., LATIN'02, Cancun, Mexico, 2002;
- Public Key Cryptography, PKC'02, Paris, France, 2002;
- The 12th Intern. Symposium on Algorithms and Computation, ISAAC'01, Christchurch, New Zealand, 2001.
- Computing: The Australasian Theory Symposium Brisbane, Australia, 2001;
- Computing: The Australasian Theory Symposium, Canberra, Australia, 2000;

Visiting Appointments.

- University of Paris-7 (06-07/2017)
- Max Planck Institute for Mathematics, Bonn (12/2016-05/2017, 04/2016,07-12/2013);
- Johann Radon Inst. for Comp. and Applied Mathematics, Linz (09/2016, 12/2013, 9/2007, 12/2006, 02/2006,04/2005, 12/2004);
- University of Paris-7 (06-07/2017)
- University of Missouri at Columbia (12/2015, 02/2005, 10/2003, 09-10/1999, 02/1998);
- University of Paris-6 (09/2015)
- University of Waterloo (05/2015, 05/2011, 09/2010, 09/2009, 01/2009, 05/2008, 03/2008, 02/2007, 07/2006, 01/2005, 08/2004, 09/1999);
- York University (05/2015);
- CIRM-Luminy, Marseille (02-7/2014);
- Darthmouth College (05/2013);
- Seoul National University, South Korea (02/2013, 11/2009, 02/2008);
- Nanyang Technological University, Singapore (02/2013, 09/2011, 04/2011, 10-11/2009, 02/2008, 02/2006);
- National University of Singapore (12/2012, 08/1998);
- Politechnic University of Catalonia, Barcelona (02/2012, 03/2007);
- University Autonoma of Madrid (02/2012, 04/2011, 03/2008);
- ENS, Paris (01-02/2012, 02-07/2010, 05/2003, 01/2001, 11/1999, 10/1996);
- Brigham Young University, Provo (02/2011);
- Royal Institute of Technology, Stockholm (09/2010, 06/1996);
- Mathematical Institute of the Czech Academy of Science (07/2010, 08/2008);
- University of Roma 3 (07/2010, 04/2002, 01/2000, 04/1998, 01/1998, 03/1996);
- Technical University of Graz (01/2010);
- Fields Institute, Toronto (09/2009, 05/2009, 11/2006, 09/2006);
- Claude Shannon Institute, University College Dublin (07/2009);
- Tsinghua University, Beijing (03/2009, 09/2006);
- EPFL, Lausanne (02/2009);
- Sogang University, South Korea (09/2008);
- Institute for Experimental Mathematics, Essen (08/2008, 11/2003);
- Inst. de Matemáticas, UNAM, Morelia, México (11/2007, 10/2003, 03/2002);
- Concordia University, Montreal (10/2007, 08/2004, 02/2004, 08/1999);
- University of Toronto (09/2007, 04/2007, 03/2006, 11/2005, 08/2004, 01/2004, 08/2003, 12/2002, 07-09/1999, 05/1997);
- Ecole Polytechnique, Paris (09/2007);
- University of Texas at Austin (04/2007);
- Technion, Haifa (03/2007, 12/1999, 12/1997);
- University of Cantabria, Santander (03/2007, 06/2004, 05-07/2003, 01-02/2003, 02/2000);
- Institute for Pure and Applied Mathematics at UCLA, Los Angeles (10/2006);
- Institute of Mathematics of the Taiwan Acad. of Sci. (06/2006, 08/1998);
- Technical University of Denmark, Copenhagen (01/2006, 06/1996);
- University of French Polynesia, Papeete (04/2005);
- NEC Labs, New Jersey (09/2004);
- University of British Columbia, Vancouver(08/2004, 02/2004, 05/1997);
- Univ. of Connecticut (05/2004, 08/2002);
- Georgia Inst. of Technology, Atlanta (03/2004);
- Sabanci Univ., Istanbul (01/2004, 12/2001);
- Royal Holloway University of London (10-12/2003, 02-03/2003, 01/1998);
- University of East Anglia, Norwich, (10/2003, 05/1995);
- University of Oxford (09-10/2003);
- Ruhr-University Bochum (12/2002);
- Institute of Computational Mathematics, Pisa (04/2002, 01/1998);

- IMPA, Rio de Janeiro (01/2002);
- University of Paris-Süd (01/2001);
- NTRU Cryptosystems (09/2000);
- University of Chile, Santiago (04/2000);
- University of Paderborn (10-12/1999, 02-07/1996, 10/1994);
- Bonn University (01/1999, 01/1997, 04/1996, 01–02/1994);
- Queensland University of Technology (07/1998);
- Institute for Inform. Processing of Austrian Acad. of Sci., Wien (01/1998, 07/1992);
- University of Western Australia (08/1997);
- University of Winnipeg (05/1997);
- University of Wisconsin at Milwaukee (04/1997);
- University of Georgia at Athens (01/1997);
- University of Aarhus (10/1996);
- Frankfurt University (07/1991);
- University of Turku (06/1996);
- Ulm University (04/1996);
- INRIA, Paris (04/1996);
- University of Saarlandes (03/1996);
- Technical University of Muenchen (02/1996);
- Penn State University (01/1996);
- University of Tasmania (01/1995, 11/1991);
- Macquarie University (10–11/1991).

Invited Lectures.

Research Centres.

- Institute of Henri Poincare, Paris, (06/2017, 09/2015, 03/2014, 02/2012);
- University of Bristol (05/2017, 02/2003);
- University of Augsburg (05/2017, 12/1999);
- University of Bielefeld (04/2017, (11/2013);
- University of Göthingen (04/2017);
- University of Basel, (03/2017, 03/2010);
- University of Lorraine, (02/2017, 4/2014);
- EPFL, Lausanne (12/2016);
- Courant Institute, NY (5/2016, 01/2001, 02/1998);
- Nanyang Technological University, Singapore (10/2015);
- ENS, Paris (09/2015, 06/2014, 02/2012);
- University of Bordeaux (09/2015, 06/2010);
- University of Paris-6 (06/2014, 05/2010, 09/2007, 01/2001, 10/1996);
- University of Heidelberg, (10/2013);
- National University of Singapore, (04/2012);
- University of Auckland (12/2010);
- ENST, Paris (02/2012);
- University of Versailles (05/2010);
- Royal Holloway University of London (12/2009, 06/2008, 02/2005);
- University of Edinburgh (06/2009, 12/2003);
- McGill University, Montreal (05/2009, 08/2008);
- Kyushu University, Fukuoka (11/2008);
- Kinki University, Fukuoka (11/2008, 10/2005);
- Niigata University, Niigata (11/2008);
- Australia National University (10/2008, 04/1997);
- University of Vienna (08/2008);

- University of California at San Diego (06/2008);
- KIAS, South Korea (06/2008, 02/2008);
- University of Calgary (05/2008, 09/2004, 05/2003);
- MIT, Boston (04/2008, 09/2000);
- University Rey Juan Carlos, Madrid (04/2008, 03/2007);
- UCLA, Los Angeles (11/2007, 02/2002);
- University of Sfax, Tunisia (08/2007);
- Postgraduate Naval School, Monterey, California (04/2007);
- Institute for Experimental Mathematics, Essen (03/2007, 01/1997);
- Frankfurt University (02/2007, 01/1999, 06/1996);
- University of Kyoto (11/2006);
- Nara Women's University (10/2006);
- NTT Labs, Yokosuka (10/2006, 08/2005);
- Tokyo Institute of Technology (10/2006, 08/2005);
- University of Karlsruhe (09/2006, 12/2002);
- University of California at Santa Barbara (09/2005);
- Harvard University (09/2005);
- University of Nagoya (09/2005);
- University of Osaka (09/2005);
- University of Klagenfurt (04/2005);
- Technical University of Graz (04/2005, 12/2004);
- Queensland University of Technology (03/2005);
- Carleton University, Ottawa (01/2004);
- Queens's University, Kingston (01/2004, 09/1999);
- King's College, London (12/2003);
- University of Cardiff (11/2003);
- University of Oviedo (07/2003);
- CWI, Amsterdam (05/2003, 01/1999);
- University of Paderborn (05/2003, 12/2002);
- University of Glasgow (02/2003);
- University of San Paulo (02/2002);
- University of Campinas (01/2002);
- Middle Eastern Techn. Univ., NY (01/2002);
- IBM T. J. Watson Research Centre (09/2000, 05/1997);
- University of Valladolid (02/2000);
- University Autonoma of Barcelona (02/2000);
- University of Rovira and Virgili, Tarragona, Catalonia (02/2000);
- University Complutense of Madrid (01/2000);
- Hebrew University, Jerusalem (01/2000, 01/1998);
- Weizmann Institute (12/1999);
- University of Tel Aviv (12/1999, 12/1997);
- University of Trier (11/1999, 01/1999);
- University of Erlangen-Nurmberg (10/1999, 02/1996);
- University of Western Ontario, London, ON (09/1999);
- International Computer Science Institute, Berkley (01/1999, 02/1998);
- University of Chicago, IL (01/1999, 4/1998);
- Bell Labs, New Jersey (01/1999, 02/1998);
- Rutgers University (10/1998);
- AT&T Research Labs (10/1998, 07/1997);
- University of Queensland (08/1998);
- University of Adelaide (06/1998);
- Stanford University (04/1998);

- Clark University, MA (04/1998);
- Buffalo University (02/1998);
- University of Wisconsin at Madison (02/1998);
- Oxford University (01/1998);
- University of Beer Sheva (12/1997);
- Curtin University of Technology of Western Australia (08/1997);
- Royal Melbourn Institute of Technology (08/1997);
- LaTrobe University at Bendigo (08/1997);
- University of Wellington (07/1997);
- Centre Commun. Research of the Inst. for Defense Analyses (05/1997);
- University of Newcastle (03/1997);
- ETH, Zurich (05/1996);
- University of Saarlandes (07/1992).

Conferences.

- *Number Theory Methods In Cryptology* Warsaw (09/2017) (invitation obtained and accepted)
- *Workshop on Efficient Congruencing and Translation-invariant Systems*, The Fields Institute, Toronto (03/2017);
- *Number Theory Down Under*, Univ. of Newcastle, Newcastle, Australia (10/2016);
- *Integers Conference*, Univ. of West Georgia, Hannover (10/2016);
- *Conference on Elementary and Analytic Number Theory*, Strobl, Austria (09/2016);
- *Analytic Number Theory and Diophantine Geometry*, Leibniz Univ., Hannover (09/2015);
- *Elementary, Analytic, and Algorithmic Number Theory: Research inspired by the mathematics of Carl Pomerance*, Univ. of University of Georgia, Athens, GA (06/2015);
- *Number Theory Down Under*, Univ. of Newcastle, Newcastle, Australia (10/2014);
- *Statistics and Number Theory September*, CRM, Montreal (09/2014);
- *Program of Dynamics and Numbers*, Max Planck Institute for Mathematics, Bonn (06/2014);
- *Workshop on Polynomials over Finite Fields*, CRM, Barcelona (05/2014);
- *Heights in Diophantine Geometry, Group Theory and Additive Combinatorics*, Erwin Schrödinger International Institute for Mathematical Physics, Vienna (11/2013);
- *Oberwolfach Meeting on Analytic Number Theory*, Oberwolfach, Germany (10/2013);
- *Erdős Centennial Conference*, Budapest, Hungary (07/2013);
- *International Workshop on Finite Fields and Their Applications*, Strobl, Austria (09/2012);
- *Workshop on Mathematical Cryptography*, CIEM, Castro Urdiales, Spain (07/2012);
- *Workshop on Quantum Cryptanalysis*, International Conference and Research Centre for Computer Science, Schloss Dagstuhl, Germany (09/2011);
- *International Conference on Applied Mathematics, Modeling and Computational Science*, Waterloo, Ontario, Canada (07/2011);
- *2nd. International Conference on Uniform Distribution Theory*, Strobl, Austria (07/2010);
- *Diophantine Approximation and Analytic Number Theory: A Tribute to Cam Stewart*, Banff, Canada (06/2010);
- *Conference Jo60: A Modern Computer Algebraist: Celebrating the Research and Influence of Joachim von zur Gathen at 60*, Bonn, Germany (05/2010);
- *Workshop on Counting Points: Theory, Algorithms and Practice*, CRM, Montreal (04/2010);
- *Workshop on Computer Security and Cryptography*, CRM, Montreal (04/2010);
- *Workshop on Graphs and Arithmetic*, CRM, Montreal (03/2010);
- *Conference on The Diverse Faces of Arithmetic*, Norwich, UK (12/2009);
- *Workshop on Quantum Algorithms and Complexity Theory*, Singapore (11/2008);
- *Workshop on Mathematical Cryptography*, Santander, Spain (10/2008);
- *Summer School on Cryptography*, Bonn, Germany (07/2008);
- *8th Central European Conference on Cryptography*, Graz, Austria (07/2008);
- *3rd Summer Workshop on Cryptography*, Seoul, South Korea (06/2008);

- *NATO Advanced Study Institute: New Challenges in Digital Communications*, Vlora, Albania (04/2008);
- *Oberwolfach Meeting on Analytic Number Theory*, Oberwolfach, Germany (03/2008);
- *International Conference on Algebraic Geometry and Coding Theory*, Luminy, France (11/2007);
- *10th Elliptic Curve Cryptography Workshop*, Toronto, Canada (09/2006);
- *4th China-Japan Conference on Number Theory*, Weihai, China (08/2006);
- *Workshop on Mathematical Cryptography*, Santander, Spain (06/2006);
- *Workshop on Boolean Functions*, International Conference and Research Centre for Computer Science, Schloss Dagstuhl, Germany (03/2006);
- *Diophantine Analysis and Related Fields*, Yokohama, Japan (03/2006);
- *Summer School on Recent Trends in Cryptography*, Santander, Spain (07/2005);
- *Workshop and Algebraic Dynamics*, UNSW, Sydney (02/2005);
- *8th Elliptic Curve Cryptography Workshop*, Bochum, Germany (09/2004);
- *36th Congress of the Mexican Mathematical Society*, Pachuca, Mexico (10/2003);
- *Workshop on Mathematics of Cryptology*, Leiden, The Netherlands (09/2003);
- *Joint Meeting of the American and Spanish Mathematical Societies, RIMS-AMS'03*, Seville, Spain (07/2003);
- *Fields Institute Conference in Number Theory in Honour of Prof. H.C. Williams*, Banff, Alberta (05/2003);
- *15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-15)*, Toulouse, France (05/2003);
- *Short Course on Cryptography, Amer. Math. Soc.*, Baltimore, MD (01/2003);
- *The 7th Spanish Meeting on Cryptology and Information Security*, Oviedo, Spain (09/2002);
- *Workshop on Mathematical Foundations of Coding Theory and Cryptology*, Singapore (07/2001);
- *The 6th International Conference on Finite Fields and their Applications*, Oaxaca, Mexico (05/2001);
- *Oberwolfach Meeting on Finite Fields and Their Applications*, Oberwolfach, Germany (01/2001);
- *Workshop on Cryptography and Computational Number Theory*, Singapore, (11/1999);
- *Missouri Algebra Weekend*, Columbia, Missouri, USA (10/1999);
- *Workshop on Algorithms and Number Theory*, International Conference and Research Centre for Computer Science, Schloss Dagstuhl, Germany (10/1998);
- *The 3rd Conference on Computational Algebra and Number Theory*, Sydney, Australia, (12/1997);
- *Oberwolfach Meeting on Finite Fields and Their Applications*, Oberwolfach, Germany (01/1997);
- *Cryptography Workshop at CWI*, Amsterdam, The Netherlands, (05/1996);
- *The 3rd International Conference on Finite Fields and their Applications*, Glasgow, UK (07/1995);
- *Workshop on Algorithms and Number Theory*, International Conference and Research Centre for Computer Science, Schloss Dagstuhl, Germany (10/1994);
- *Workshop on Algebraic Complexity and Parallelism* , International Conference and Research Centre for Computer Science, Schloss Dagstuhl, Germany (07/1992);
- *International Conference on Analytic and Probabilistic Methods in Number Theory*, Palanga, Lithuanian, (9/1991);
- *French-Soviet Workshop on Coding Theory*, Paris, France (07/1991);
- *International Conference on Algebraic Geometry and Coding Theory*, Luminy, France (06/1991);
- *International Conference on Computer Algebra in Physical Researches*, Dubna, USSR (07/1990);
- *All-Union Conference on Constructive Methods and Algorithms of Number Theory*, Minsk, USSR (09/1989);
- *All-Union Conf. on Transcendental Numbers and their Applications*, Moscow, USSR (10/1983).