List of talks

Daniel J. Bernstein
djb@cr.yp.to

2008.10.05

This is a chronological list of the talks that I've given. Each entry in the list includes date, duration (when known), type, audience type, country, and further details. There are several audience types: "researchers" means a talk for researchers who travelled to a conference; "students" means a talk for students who travelled to a conference; "local" means a talk in a seminar, colloquium, etc. Regular course lectures aren't listed here. Some statistics:

- 187 talks given. 143 with slides online. 9 with audio online.
- 145 invited talks (29 for students at conferences, 74 for researchers at conferences, 42 seminars/colloquia/etc.); 17 refereed talks; 28 contributed talks.
- 138 invited talks of known length, averaging 53 minutes.
- Lecture locations, by country: 4 Australia. 4 Austria. 2 Belgium. 5 Brazil. 18 Canada. 1 China. 6 Denmark. 4 England. 7 France. 14 Germany. 3 Greece. 3 India. 4 Ireland. 1 Japan. 3 Luxembourg. 1 Malaysia. 1 Morocco. 12 Netherlands. 4 Poland. 2 Russia. 1 South Korea. 4 Spain. 2 Switzerland. 5 Taiwan. 2 Turkey. 77 USA.

See `http://cr.yp.to/talks.html` for abstracts, slides, audio, etc.

1987.06.01 10 minutes contributed talk researchers USA
Ramanujan Centenary Conference. University of Illinois at Urbana-Champaign. "New fast algorithms for π and e."

1992.12 contributed talk researchers USA
West Coast Number Theory Conference. Oregon State University, Corvallis. $3x + 1$ results.

1992.12 contributed talk researchers USA
West Coast Number Theory Conference. Oregon State University, Corvallis. Computing Dickman's ρ function.

1994.05.02 45 minutes invited talk researchers Canada
Computational Number Theory. Fields Institute, Waterloo, Ontario. "Practical aspects of the number field sieve."

1994.10.12 invited talk researchers Germany
Algorithms and Number Theory. Schloss Dagstuhl. Preliminary report on detecting perfect powers.

1995.02.06 invited talk local researchers USA
Seminar, Department of Mathematics, Texas A&M University, College Station, Texas. Detecting perfect powers.

1995.03.01 50 minutes invited talk local researchers USA
Colloquium, Department of Mathematics, Statistics, and Computer Science. University of Illinois at Chicago. Detecting perfect powers.

1995.04.05 50 minutes invited talk local researchers USA
Number Theory Seminar, Department of Mathematics, University of California at Berkeley. "Detecting perfect powers."

1995.05 invited talk researchers Germany
Computational Number Theory. Mathematisches Forschungsinstitut, Oberwolfach. Multidigit modular multiplication with ECRT.

1995.10.03 50 minutes invited talk local researchers USA
Seminar, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago. Survey of topics related to number field sieve.

1995.10.17 50 minutes invited talk local researchers USA
Number Theory Seminar, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago. Generalized Gaussian elimination.

1995.11.15 50 minutes invited talk local researchers USA
Computer Science Seminar, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago. Universal pattern-matching automaton.

1995.12.02 40 minutes invited talk researchers USA
Midwest Algebraic Number Theory Day III. University of Michigan, Ann Arbor. "Fast ideal arithmetic via lazy localization."

1996.05.22 20 minutes refereed talk researchers France
Algorithmic Number Theory Symposium (ANTS) II. University of Bordeaux. "Fast ideal arithmetic via lazy localization."

1997.03.07 30 minutes invited talk researchers USA
Mathematics of Cryptography and Security. Southwest Regional Institute in the Mathematical Sciences (SWRIMS), University of Arizona, Tucson. "The world's fastest digital signature system."

1997.03.17 50 minutes invited talk local researchers USA
Seminar, Department of Mathematics and Computer Science, Butler University. "The world's fastest digital signature system."

1997.05.30 invited talk researchers Germany
Computational Aspects of Commutative Algebra and Algebraic Geometry. Schloss Dagstuhl. "Composing power series over a finite ring in essentially linear time."

1997.10.25 20 minutes invited talk researchers USA
Special Session on Number Theory and Cryptography; Central Section Meeting, American Mathematical Society (AMS). University of Wisconsin at Milwaukee. "A secure digital signature system with verification ten times faster than RSA."

1997.11.19 50 minutes invited talk local researchers USA
Number Theory Seminar, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago. "Factoring into coprimes in essentially linear time."

1997.12.03 50 minutes invited talk local researchers USA
Number Theory Seminar, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago. "Improving on the Sieve of Eratosthenes," talk given jointly with A. O. L. Atkin.

1998.02.13 50 minutes invited talk local researchers USA
Colloquium, Department of Mathematics, Statistics, and Computer Science. University of Illinois at Chicago. "Computing everything in essentially linear time."

1998.06.21 20 minutes refereed talk researchers USA
Algorithmic Number Theory Symposium (ANTS) III. Reed College, Portland, Oregon. "Bounding smooth integers."

1998.09.12 invited talk researchers USA
Special Session on Number Theory; Central Section Meeting, American Mathematical Society (AMS). DePaul University, Chicago, Illinois. "Estimating the speed of the quadratic sieve (preliminary report)."

1998.10.29 30 minutes invited talk researchers Germany
Algorithms and Number Theory. Schloss Dagstuhl. "Ten topics in computational number theory."

1999.02.23 50 minutes invited talk local faculty USA
Mathematics in Science and Society Seminar, Department of Mathematics, University of Illinois at Urbana-Champaign. "How to become an international arms dealer."

1999.02.23 50 minutes invited talk local researchers USA
Number Theory Seminar, Department of Mathematics, University of Illinois at Urbana-Champaign. "Fast, arbitrarily precise computation of Psi."

1999.06.13 20 minutes contributed talk researchers Canada
The Mathematics of Public-Key Cryptography. Fields Institute, Toronto, Ontario. "Guaranteed message authentication faster than MD5."

1999.07.06 invited talk researchers Germany
Explicit Methods in Number Theory. Mathematisches Forschungsinstitut, Oberwolfach. "Counting rational points by brute force."

1999.10.13 10:45 40 minutes invited talk researchers China
Workshop on Complexity of Equation Solving and Algebra, Foundations of Computational Mathematics. City University of Hong Kong. "Solving equations to high precision."

2000.04.08 20 minutes invited talk researchers USA
Special Session on Number Theory, Algorithms, and Cryptography; Central Section Meeting, American Mathematical Society (AMS). University of Notre Dame, Indiana. "Faster multiplication of integers."

2000.05.22 30 minutes invited talk researchers USA
Millennial Conference in Number Theory. University of Illinois at Urbana-Champaign. "Arbitrarily precise bounds on the distribution of smooth integers."

2000.06.10 25 minutes invited talk researchers Canada
Session on Cryptography and Number Theory, Canadian Mathematical Society summer meeting, MATH 2000. McMaster University, Hamilton, Ontario. "Sieving in cache."

2000.06.27 30 minutes invited talk researchers Russia
Session on Algebraic Algorithms and Complexity, 6th IMACS Conference on Applications of Computer Algebra (ACA). Shuvalov Palace, St. Petersburg. "High-precision high-degree polynomial factorization (preliminary report)."

2000.07.27 50 minutes invited talk researchers England
London Mathematical Society (LMS) Durham Symposium on Computational Number Theory. University of Durham. "Rethinking the number field sieve."

2000.08.14 60 minutes invited talk researchers USA
Clay Mathematics Institute Introductory Workshop in Algorithmic Number Theory. Mathematical Sciences Research Institute, Berkeley, California. "Fast multiplication."

2000.08.15 60 minutes invited talk researchers USA
Clay Mathematics Institute Introductory Workshop in Algorithmic Number Theory. Mathematical Sciences Research Institute, Berkeley, California. "Applications of fast multiplication."

2000.08.18 60 minutes invited talk researchers USA
Clay Mathematics Institute Introductory Workshop in Algorithmic Number Theory. Mathematical Sciences Research Institute, Berkeley, California. "Protecting communications against forgery."

2000.09.07 50 minutes invited talk local researchers USA
Colloquium, Department of Mathematics, University of California at Berkeley. "Factoring into coprimes."

2000.10.06 48 minutes invited talk local researchers USA
Number Theory Seminar, Department of Mathematics, University of California at Berkeley. "Arbitrarily precise bounds on smooth integers."

2000.10.20 60 minutes invited talk researchers USA
Number-Theoretic Cryptography. Mathematical Sciences Research Institute, Berkeley, California. "Design and implementation of a public-key signature system."

2001.03.23 50 minutes invited talk local researchers USA
Seminar, Computer Science Department, Butler University. "The NSA sieving circuit."

2001.05.07 6 minutes contributed talk researchers Austria
Eurocrypt 2001. Innsbruck. “The NSA sieving circuit.”

2001.05.14 40 minutes invited talk researchers Germany
Algorithms and Number Theory. Schloss Dagstuhl. “An introduction to Schimmler sorting.”

2001.06.13 45 minutes invited talk local researchers USA
Seminar, Cambridge Research Laboratory, Compaq Computer Corporation, Cambridge, Massachusetts. “The state of the art in RSA-type signatures.”

2001.07.27 35 minutes invited talk researchers Germany
Explicit Methods in Number Theory. Mathematisches Forschungsinstitut, Oberwolfach. “Finding polynomial values of small height.”

2001.09.22 30 minutes invited talk researchers USA
Special Session on Cryptography and Computational and Algorithmic Number Theory; Central Section Meeting, American Mathematical Society (AMS). Ohio State University, Columbus. “Elliptic curve cryptography: the case of NIST P-224.”

2001.10.29 60 minutes invited talk researchers Canada
Elliptic Curve Cryptography (ECC) 2001. University of Waterloo, Ontario. “A software implementation of NIST P-224.”

2001.11.02 60 minutes invited talk researchers USA
Midwest Arithmetical Geometry in Cryptography (MAGC). University of Illinois at Urbana-Champaign. “A complete software implementation of NIST P-224.”

2002.01.28 50 minutes invited talk local researchers USA
Colloquium, Department of Mathematics, University of Pittsburgh. “Is a 2048-bit factorization worth $200,000?”

2002.04.24 50 minutes invited talk local researchers USA
Mathematics and Applications Seminar, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago. “Finding roots of high-degree polynomials.”

2002.06.15 25 minutes invited talk researchers Canada
Symposium on Cryptography; 2002 Summer Meeting, Canadian Mathematical Society (CMS). University of Laval, Quebec. “Speed records for cryptographic software: an update.”

2002.08.20 10 minutes invited talk researchers USA
Crypto 2002. Santa Barbara. “Deterministic polynomial-time primality tests.”

2002.08.20 5 minutes contributed talk researchers USA
Crypto 2002. Santa Barbara. “The cost of integer factorization.”

2002.10.31 50 minutes invited talk local researchers USA
Colloquium, Department of Mathematics, University of California at Berkeley. “Proving primality.”

2003.02.11 60 minutes invited talk local researchers USA
Security Seminar, Computer Science Department, Stanford University. “The DNS security mess.”

2003.03.18 60 minutes invited talk local researchers USA
Seminar, Sun Microsystems. “The DNS security mess.”

2003.03.23 09:30 45 minutes invited talk researchers USA
Lenstra Treurfeest. “A new proof that 83 is prime.”

2003.03.25 15:45 60 minutes invited talk researchers USA
Future directions in algorithmic number theory. American Institute of Mathematics, Palo Alto, California. “Randomized primality proving in essentially quartic time.”

2003.03.26 11:30 30 minutes invited talk researchers USA
Future directions in algorithmic number theory. American Institute of Mathematics, Palo Alto, California. “Rethinking the number-field sieve: an update.”

2003.04.03 14:00 50 minutes invited talk local researchers USA
Algebraic Number Theory Seminar, Department of Mathematics, University of Illinois at Urbana-Champaign. “Sharper ABC-based bounds for congruent polynomials.”

2003.04.04 15:30 45 minutes invited talk researchers USA
Special Session on Cryptography and Computational and Algorithmic Number Theory; Central Section Meeting, American Mathematical Society (AMS). Indiana University, Bloomington. “Randomized primality proving in essentially quartic time.”

2003.04.24 08:00 75 minutes invited talk local students USA
Class talk, Butler University. “Compressing RSA keys and signatures.”

2003.05.03 17:00 40 minutes invited talk researchers USA
Special Session on Geometry and Arithmetic over Finite Fields; Western Section Meeting, American Mathematical Society (AMS). San Francisco, California. “Sharper ABC-based bounds for congruent polynomials.”

2003.05.10 invited talk researchers USA
Midwest Algebraic Number Theory Day. “Sharper ABC-based bounds for congruent polynomials.”

2003.05.26 11:00 30 minutes invited talk researchers Canada
Conference in Number Theory in Honour of Professor H. C. Williams. Banff Centre, Alberta. “Doubly focused enumeration of locally square polynomial values.”

2003.07.24 20 minutes contributed talk researchers Germany
Explicit Methods in Number Theory. Mathematisches Forschungsinstitut, Oberwolfach. “Translating Chudnovsky into English.”

2003.11.08 15:10 20 minutes contributed talk researchers USA
Mathematics of Public Key Cryptography (MPKC) 2003. University of Illinois at Chicago. “News from the Rabin-Williams front.”

2003.11.08 16:40 20 minutes contributed talk researchers USA
Mathematics of Public Key Cryptography (MPKC) 2003. University of Illinois at Chicago. “More news from the Rabin-Williams front.”

2004.04.28 11:00 50 minutes invited talk local researchers USA
Special Seminar, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign. “The DNS security mess.”

2004.05.14 09:00 30 minutes invited talk researchers USA
Special Session on Coding Theory and Cryptography; Sixth International Joint Meeting, American Mathematical Society (AMS) and Sociedad Matematica Mexicana. Hyatt Regency Houston, Texas. “How to find smooth parts of integers.”

2004.06.14 09:00 60 minutes invited talk researchers USA
Algorithmic Number Theory Symposium (ANTS) VI. University of Vermont, Burlington. “Factorization myths.”

2004.06.24 10:20 25 minutes invited talk researchers Canada
Special Session on Computational Number Theory; Canadian Number Theory Association (CNTA) VIII. University of Toronto, Ontario. “Doubly focused enumeration in two dimensions.”

2004.07.07 11:00 60 minutes invited talk researchers Australia
Polynomial-Based Cryptography. University of Melbourne. “How to find smooth parts of integers.”

2004.07.29 15:00 60 minutes invited talk local researchers Australia
Computational Algebra Seminar, School of Mathematics and Statistics, University of Sydney. “Factorization myths.”

2004.08.17 20:35 5 minutes contributed talk researchers USA
Crypto 2004. Santa Barbara. “Stop overestimating RSA bandwidth!”

2004.09.16 15:00 60 minutes invited talk local students USA
Colloquium aimed at graduate students, University of Illinois at Chicago. “A state-of-the-art public-key signature system.”

2004.11.15 14:00 60 minutes invited talk researchers Canada
Explicit Methods in Number Theory. Banff Centre, Alberta. “Three algorithms related to the number-field sieve.”

2004.11.19 14:00 50 minutes invited talk local researchers Canada
Discrete Math Seminar, Department of Mathematics and Statistics, University of Calgary. “Faster factorization into coprimes.”

2005.02.15 14:00 50 minutes invited talk local researchers USA
Computer Security Seminar, Department of Computer Science, University of Illinois at Chicago. “The Poly1305-AES message-authentication code.”

2005.02.21 10:05 25 minutes refereed talk researchers France
Fast Software Encryption (FSE) 2005. Paris. “The Poly1305-AES message-authentication code.”

2005.02.21 16:52 4 minutes contributed talk researchers France
Fast Software Encryption (FSE) 2005. Paris. “Have any challenges for qhasm?”

2005.02.25 09:00 60 minutes invited talk researchers France
Special-purpose Hardware for Attacking Cryptographic Systems (SHARCS). Paris. “Building circuits for integer factorization.”

2005.04.26 16:00 15 minutes invited talk local faculty USA
University of Illinois at Chicago. On panel responding to 2005 Nakata Lecture by R. Michael Tanner.

2005.05.19 14:00 50 minutes invited talk local researchers Denmark
Seminar, Department of Mathematics, Technical University of Denmark, Copenhagen. “High-speed elliptic-curve cryptography.”

2005.05.23 16:10 25 minutes refereed talk researchers Denmark
Eurocrypt 2005. Scandinavian Congress Center, Aarhus. “Stronger security bounds for Wegman-Carter-Shoup authenticators.”

2005.05.26 14:15 12 minutes refereed talk researchers Denmark
ECRYPT STVL Workshop on Symmetric Key Encryption (SKEW 2005). Scandinavian Congress Center, Aarhus. “The Salsa20 stream cipher.”

2005.05.27 10:45 12 minutes refereed talk researchers Denmark
ECRYPT STVL Workshop on Symmetric Key Encryption (SKEW 2005). Scandinavian Congress Center, Aarhus. “Understanding brute force.”

2005.05.30 11:00 90 minutes invited talk researchers Poland
Quo Vadis Cryptology? Advances in Cryptanalysis. Warsaw, Poland. “The power of parallel computation.”

2005.06.01 09:00 40 minutes invited talk researchers Poland
ENIGMA 2005. Warsaw, Poland. “Cache-timing attacks on AES.”

2005.06.11 10:30 60 minutes invited talk researchers USA
CAM 2005. University of Central Oklahoma, Edmond, Oklahoma. “The power of parallel computation.”

2005.06.11 14:40 45 minutes invited talk researchers USA
CAM 2005. University of Central Oklahoma, Edmond, Oklahoma. “Integer factorization.”

2005.07.08 16:00 45 minutes invited talk researchers Spain
Computational Number Theory Workshop; Foundations of Computational Mathematics (FoCM) 2005. Universidad de Cantabria, Santander, Spain. “Integer factorization: a progress report.”

2005.07.19 10:45 25 minutes invited talk researchers Germany
Explicit Methods in Number Theory. Mathematisches Forschungsinstitut, Oberwolfach. “Polynomial selection for the number-field sieve, part 2: polynomial merit.”

2005.09.19 20:00 5 minutes contributed talk researchers Denmark
Elliptic Curve Cryptography (ECC) 2005. Denmark Technical University, Copenhagen. “Is $2^{255} - 19$ big enough?”

2005.09.20 09:30 60 minutes invited talk researchers Denmark
Elliptic Curve Cryptography (ECC) 2005. Denmark Technical University, Copenhagen. “New speed records for point multiplication.”

2005.11.06 19:40 50 minutes invited talk researchers Canada
Number Theory Inspired By Cryptography (NTIBC) 2005. Banff Centre, Alberta, Canada. “Compressing RSA/Rabin keys.”

2006.02.02 14:25 20 minutes refereed talk researchers Belgium
SASC 2006 - Stream Ciphers Revisited. College De Valk, Leuven, Belgium. “Comparison of 256-bit stream ciphers.”

2006.03.11 14:30 50 minutes invited talk students USA
Arizona Winter School 2006. University of Arizona, Tucson, Arizona. “Integer factorization, part 1: the Q sieve.”

2006.03.12 16:00 50 minutes invited talk students USA
Arizona Winter School 2006. University of Arizona, Tucson, Arizona. “Integer factorization, part 2: detecting smoothness.”

2006.03.13 16:00 50 minutes invited talk students USA
Arizona Winter School 2006. University of Arizona, Tucson, Arizona. “Integer factorization, part 3: the number-field sieve.”

2006.03.14 10:00 50 minutes invited talk students USA
Arizona Winter School 2006. University of Arizona, Tucson, Arizona. “Integer factorization, part 4: polynomial selection.”

2006.04.03 17:30 6 minutes contributed talk researchers Germany
SHARCS 2006. Dorint Kongress Hotel, Cologne. “eBATS: ECRYPT Benchmarking of Asymmetric Systems.”

2006.04.09 15:30 20 minutes invited talk researchers USA
Special Session on Number Theory; Central Section Meeting, American Mathematical Society. University of Notre Dame, Indiana. “Differential addition chains.”

2006.04.25 09:50 25 minutes refereed talk researchers USA
PKC 2006. Columbia University, New York. “Curve25519: new Diffie-Hellman speed records.”

2006.05.30 19:50 4 minutes contributed talk researchers Russia
Eurocrypt 2006. Pulkovskaya Hotel, St. Petersburg. “eBATS: ECRYPT Benchmarking of Asymmetric Systems.”

2006.06.15 16:15 105 minutes invited talk students Belgium
Summer School on Cryptographic Hardware, Side-Channel and Fault Attacks. Louvain-la-Neuve. “Cache-timing attacks.”

2006.06.26 09:50 80 minutes invited talk students USA
Summer School on Computational Number Theory and Applications to Cryptography. University of Wyoming, Laramie. “The number-field sieve.”

2006.06.27 09:50 80 minutes invited talk students USA
Summer School on Computational Number Theory and Applications to Cryptography. University of Wyoming, Laramie. “Finding small factors of integers.”

2006.06.28 09:50 80 minutes invited talk students USA
Summer School on Computational Number Theory and Applications to Cryptography. University of Wyoming, Laramie. “Speed of the number-field sieve.”

2006.06.29 09:50 80 minutes invited talk students USA
Summer School on Computational Number Theory and Applications to Cryptography. University of Wyoming, Laramie. “Proving primality in polynomial time.”

2006.06.30 09:50 80 minutes invited talk students USA
Summer School on Computational Number Theory and Applications to Cryptography. University of Wyoming, Laramie. “Proving primality more quickly.”

2006.07.10 10:00 30 minutes invited talk researchers Australia
31st Australasian Conference on Combinatorial Mathematics and Combinatorial Computing. Voyages Resort, Alice Springs. “Differential addition chains.”

2006.08.03 10:00 50 minutes invited talk researchers Japan
2006 Workshop on Cryptography and Related Mathematics. Chuo University, Tokyo. “High-speed cryptographic functions.”

2006.08.14 13:30 50 minutes invited talk students Taiwan
Information Security Summer School (ISSS) 2006. Taipei. “Efficient arithmetic in finite fields.”

2006.08.15 09:30 50 minutes invited talk students Taiwan
Information Security Summer School (ISSS) 2006. Taipei. “Elliptic curves.”

2006.08.15 14:30 50 minutes invited talk students Taiwan
Information Security Summer School (ISSS) 2006. Taipei. “Efficient arithmetic on elliptic curves.”

2006.08.16 11:40 50 minutes invited talk students Taiwan
Information Security Summer School (ISSS) 2006. Taipei. “Choosing curves.”

2006.08.28 14:30 50 minutes invited talk researchers Brazil
6th Brazilian Symposium on Information and Computer System Security (SBSeg ’06). Mendes Convention Center, Santos. “The DNS security mess.”

2006.08.30 13:30 60 minutes invited talk students Brazil
Workshop on Cryptographic Algorithms and Protocols (WCAP 2006). Mendes Convention Center, Santos. “Efficient arithmetic in finite fields.”

2006.08.30 14:30 60 minutes invited talk students Brazil
Workshop on Cryptographic Algorithms and Protocols (WCAP 2006). Mendes Convention Center, Santos. “Elliptic curves.”

2006.08.31 13:30 60 minutes invited talk students Brazil
Workshop on Cryptographic Algorithms and Protocols (WCAP 2006). Mendes Convention Center, Santos. “Efficient arithmetic on elliptic curves.”

2006.08.31 14:30 60 minutes invited talk students Brazil
Workshop on Cryptographic Algorithms and Protocols (WCAP 2006). Mendes Convention Center, Santos. “Choosing curves.”

2006.09.11 09:00 60 minutes invited talk students Canada
Summer School on Elliptic and Hyperelliptic Curve Cryptography. Fields Institute, Toronto, Ontario. “Efficient arithmetic in finite fields.”

2006.09.13 09:00 60 minutes invited talk students Canada
Summer School on Elliptic and Hyperelliptic Curve Cryptography. Fields Institute, Toronto, Ontario. “Efficient arithmetic on elliptic curves in large characteristic.”

2006.09.20 11:10 50 minutes invited talk researchers Canada
Elliptic Curve Cryptography (ECC) 2006. Fields Institute, Toronto, Canada. “Elliptic vs. hyperelliptic, part 1.”

2006.10.17 13:00 50 minutes invited talk local researchers Canada
Distinguished Lecture, Institute for Computer Research, University of Waterloo. “The DNS security mess.”

2006.11.19 17:00 30 minutes contributed talk researchers Canada
Polynomials over Finite Fields and Applications. Banff Centre, Alberta, Canada. “Faster factorization into coprimes.”

2006.11.27 14:10 50 minutes invited talk researchers Canada
Workshop on Cryptography: Underlying Mathematics, Provability and Foundations. Fields Institute, Toronto, Canada. “Proving tight security for Rabin-Williams signatures.”

2006.12.10 11:30 90 minutes invited talk students India
Tutorial session; INDOCRYPT 2006. Park Hotel, Kolkata, India. “High-speed Diffie-Hellman, part 1.”

2006.12.10 15:45 90 minutes invited talk students India
Tutorial session; INDOCRYPT 2006. Park Hotel, Kolkata, India. “High-speed Diffie-Hellman, part 2.”

2007.01.31 14:15 15 minutes refereed talk researchers Germany
SASC 2007—The State of the Art of Stream Ciphers. Ruhr University Bochum. “Cycle counts for authenticated encryption.”

2007.02.02 15:00 45 minutes invited talk local researchers Netherlands
EIDMA/DIAMANT Cryptography Working Group. Universiteit van Amsterdam. “The DNS security mess.”

2007.02.07 12:00 60 minutes invited talk local researchers England
The Enigma Variations: Information Security Seminar. Bristol University. “Proving tight security for Rabin-Williams signatures.”

2007.02.08 13:00 contributed talk researchers England
ECRYPT VAMPIRE WG1. Bristol University. “High-speed engineering of high-speed software.”

2007.03.20 11:00 90 minutes invited talk local researchers USA
Colloquium, Akamai Technologies. “The DNS security mess.”

2007.04.17 09:00 50 minutes invited talk researchers USA
Workshop on Complexity, Coding, and Communications. Institute for Mathematics and its Applications, University of Minnesota, Minneapolis. “The tangent FFT.”

2007.04.25 14:30 60 minutes invited talk local researchers Netherlands
EIDMA Seminar Combinatorial Theory. Technische Universiteit Eindhoven. “Elliptic vs. hyperelliptic, part 1.”

2007.04.27 14:15 165 minutes invited talk local students Germany
Hackerpraktikum. Horst Görtz Institut für Sicherheit in der Informationstechnik, Ruhr-Universität Bochum. “How to program secure network servers.”

2007.04.30 11:35 70 minutes invited talk students Greece
Emerging Topics in Cryptographic Design and Cryptanalysis. Doryssa Seaside Resort, Pythagorion, Samos. “On the design of message-authentication codes.”

2007.05.04 16:20 70 minutes invited talk students Greece
Emerging Topics in Cryptographic Design and Cryptanalysis. Doryssa Seaside Resort, Pythagorion, Samos. “CPU traps and pitfalls.”

2007.05.15 16:30 60 minutes invited talk local researchers Netherlands
Algemeen Wiskunde Colloquium. Department of Mathematics and Computer Science, Technische Universiteit Eindhoven. “Circuits for integer factorization.”

2007.05.18 14:30 40 minutes invited talk researchers USA
Number Theory Fest. Department of Mathematics, University of Illinois at Urbana-Champaign. “Distinguishing prime numbers from composite numbers: the state of the art.”

2007.05.22 20:27 6 minutes contributed talk researchers Spain
Eurocrypt 2007. Catalonia Barcelona Plaza Hotel, Barcelona. “Elliptic vs. hyperelliptic, part 3: Elliptic strikes back.” Talk given jointly with Tanja Lange.

2007.05.24 17:20 25 minutes refereed talk researchers Spain
ECRYPT Hash Workshop 2007. Universitat Oberta de Catalunya, Barcelona. “What output size resists collisions in a xor of independent expansions?”

2007.05.28 15:05 75 minutes invited talk researchers Poland
Quo vadis cryptology? Threat of side-channel attacks. LORD Hotel, Warsaw. “The impact of side-channel attacks on the design of cryptosystems.”

2007.06.07 14:00 60 minutes invited talk researchers USA
Mathfest 2007. National Security Agency, Fort Meade, Maryland. “Edwards coordinates for elliptic curves.”

2007.06.11 14:30 60 minutes invited talk researchers Netherlands
Software Performance Enhancement for Encryption and Decryption (SPEED). Victoria Hotel, Amsterdam. “How fast is cryptography?”

2007.06.11 17:05 10 minutes contributed talk researchers Netherlands
Software Performance Enhancement for Encryption and Decryption (SPEED). Victoria Hotel, Amsterdam. “Elliptic vs. hyperelliptic, part 3: Elliptic strikes back.” Talk given jointly with Tanja Lange.

2007.07.12 12:15 25 minutes contributed talk researchers Australia
8th International Conference on Finite Fields and Applications (FQ8). Amora Hotel Riverwalk Melbourne, Richmond. “Polynomial evaluation and message authentication.”

2007.07.18 10:15 20 minutes invited talk researchers Germany
Explicit Methods in Number Theory. Mathematisches Forschungsinstitut, Oberwolfach. “Complexity news: FFTs and integer multiplication.”

2007.08.16 11:35 55 minutes invited talk researchers Canada
Selected Areas in Cryptography (SAC) 2007. University of Ottawa, Ontario. “Edwards coordinates for elliptic curves.”

2007.09.03 09:30 60 minutes invited talk students Ireland
Tutorial on Elliptic and Hyperelliptic Curve Cryptography 2007. University College Dublin. “Elliptic curves over $\mathbf{R}$ and $\mathbf{F}_q$.”

2007.09.03 12:00 60 minutes invited talk students Ireland
Tutorial on Elliptic and Hyperelliptic Curve Cryptography 2007. University College Dublin. “Generic attacks and index calculus.”

2007.09.05 17:52 8 minutes contributed talk researchers Ireland
Elliptic Curve Cryptography (ECC) 2007. University College Dublin. “The Explicit-Formulas Database.”

2007.09.07 11:40 50 minutes invited talk researchers Ireland
Elliptic Curve Cryptography (ECC) 2007. University College Dublin. “Elliptic vs. hyperelliptic, part 3: Elliptic strikes back.” Talk given jointly with Tanja Lange.

2007.09.10 11:30 30 minutes refereed talk researchers Austria
Special-purpose Hardware for Attacking Cryptographic Systems (SHARCS) 2007. Vienna Marriott Hotel. “Better price-performance ratios for generalized birthday attacks.”

2007.09.10 15:07 2 minutes contributed talk researchers Austria
Special-purpose Hardware for Attacking Cryptographic Systems (SHARCS) 2007. Vienna Marriott Hotel. “Edwards curves.”

2007.09.11 19:50 5 minutes contributed talk researchers Austria
Cryptographic Hardware and Embedded Systems (CHES) 2007. Vienna Marriott Hotel. “The EFD thing.” Talk given jointly with Tanja Lange.

2007.09.24 11:50 25 minutes refereed talk researchers Poland
ECRYPT Workshop on Tools for Cryptanalysis. Conference Center of the Jagiellonian University in Kraków-Przegorzay. “Cipher DAGs.”

2007.10.19 15:00 50 minutes invited talk researchers France
Explicit Methods in Number Theory. Universite Bordeaux I. “Edwards coordinates for elliptic curves, part 2.”

2007.11.02 08:30 60 minutes invited talk researchers USA
1st Computer Security Architecture Workshop. George Mason University, Fairfax, Virginia. “Some thoughts on security after ten years of qmail 1.0.”

2007.11.10 16:30 30 minutes invited talk researchers England
SAGE Days 6. University of Bristol. “Edwards coordinates for elliptic curves, part 2.”

2007.11.30 15:10 50 minutes invited talk researchers South Korea
ICISC 2007. Seoul. “High-speed cryptography.”

2007.12.03 09:50 25 minutes refereed talk researchers Malaysia
Asiacrypt 2007. Crowne Plaza Riverside, Kuching, Sarawak. “Faster addition and doubling on elliptic curves.” Talk given jointly with Tanja Lange.

2007.12.17 09:00 50 minutes invited talk researchers India
Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17). Indian Institute of Science, Bangalore. “The tangent FFT.”

2007.12.24 15:00 80 minutes invited talk local students Taiwan
Electrical Engineering seminar. National Taiwan University. “An introduction to high-speed arithmetic.”

2008.01.09 17:30 5 minutes contributed talk researchers Luxembourg
Echternach Symmetric Cryptography (ESC) Seminar. Hotel Bel-Air, Echternach. “ChaCha20.”

2008.01.09 17:35 5 minutes contributed talk researchers Luxembourg
Echternach Symmetric Cryptography (ESC) Seminar. Hotel Bel-Air, Echternach. “MAC1271.”

2008.01.11 10:40 20 minutes invited talk researchers Luxembourg
Echternach Symmetric Cryptography (ESC) Seminar. Hotel Bel-Air, Echternach. “Cipher DAGs.”

2008.02.12 17:16 4 minutes contributed talk researchers Switzerland
Fast Software Encryption 2008. Moevenpick Hotel, Lausanne. “SHARCS vs. SWIFFT.”

2008.02.14 10:45 15 minutes refereed talk researchers Switzerland
State of the Art of Stream Ciphers (SASC) 2008. Moevenpick Hotel, Lausanne. “ChaCha, a variant of Salsa20.”

2008.04.14 11:25 25 minutes refereed talk researchers Turkey
Eurocrypt 2008. Hilton Hotel Convention Center, Istanbul. “Proving tight security for Rabin–Williams signatures.”

2008.04.15 20:21 4 minutes contributed talk researchers Turkey
Eurocrypt 2008. Hilton Hotel Convention Center, Istanbul. “Binary Edwards curves.”

2008.04.18 15:30 50 minutes invited talk local researchers Netherlands
Intercity Number Theory Seminar: genus 2 day. Universiteit Utrecht. “Hyperelliptic-curve cryptography.”

2008.04.23 09:00 60 minutes invited talk researchers Germany
Troopers08. Kempinski Airport Hotel, Munich. “Invulnerable software.”

2008.05.09 12:30 60 minutes invited talk local researchers Spain
Algebra and Number Theory Seminar. Department of Mathematics, Universidad Autonomo de Madrid. “Binary Edwards curves.” Talk given jointly with Tanja Lange.

2008.05.12 14:50 70 minutes invited talk students Greece
ECRYPT Summer School on Advanced Topics in Cryptography. Fodele Beach Hotel, Crete, Greece. “The rest of the zoo.”

2008.05.19 16:50 10 minutes contributed talk researchers Canada
Algorithmic Number Theory Symposium (ANTS). Banff Centre, Alberta. “The elliptic-curve zoo: a study of curve shapes.” Talk given jointly with Tanja Lange.

2008.06.05 09:30 90 minutes invited talk researchers Netherlands
Hash functions in cryptology: theory and practice. Lorentz Center, Leiden University. “How fast are hash functions?” Keynote talk.

2008.06.13 15:00 30 minutes refereed talk researchers Morocco
Africacrypt 2008. Casablanca. “Twisted Edwards curves.”

2008.06.20 14:30 60 minutes invited talk local researchers France
Seminar, University of Rennes. “The elliptic-curve zoo.”

2008.07.17 15:25 45 minutes invited talk researchers Netherlands
Beeger Lecture, 5th European Congress of Mathematics (5ECM). RAI Amsterdam. “Edwards curves.”

2008.08.12 16:45 25 minutes refereed talk researchers USA
Cryptographic Hardware and Embedded Systems 2008 (CHES 2008). Renaissance Mayflower Hotel. “Binary Edwards curves.” Talk given jointly with Tanja Lange.

2008.08.22 14:00 60 minutes invited talk local researchers USA
Seminar, Department of Computer Science. University of Illinois at Chicago. “DNSCurve: Usable security for DNS.”

2008.09.15 11:45 60 minutes invited talk students Netherlands
DIAMANT Summer School on Elliptic and Hyperelliptic Curve Cryptography. Technische Universiteit Eindhoven. “Introduction to elliptic curves.”

2008.09.17 11:45 60 minutes invited talk students Netherlands
DIAMANT Summer School on Elliptic and Hyperelliptic Curve Cryptography. Technische Universiteit Eindhoven. “Fast arithmetic on elliptic curves.”

2008.09.22 19:50? 5 minutes contributed talk researchers Netherlands
The 12th Workshop on Elliptic Curve Cryptography (ECC 2008). “DNSCurve: Usable security for DNS.”

2008.10.07 14:30 60 minutes invited talk (planned) researchers France
Cado Workshop on Integer Factorization. LORIA, Nancy. “Predicting NFS time.”

2008.10.10 16:00 60 minutes invited talk (planned) researchers Netherlands
Lustrum OS3. Turingzaal, CWI, Amsterdam. “Internet security.”

2008.10.18 09:00 60 minutes invited talk (planned) researchers USA
The Second International Workshop on Post-Quantum Cryptography (PQCrypto 2008). University of Cincinnati. “Survey of post-quantum cryptography.”