Curriculum Vita

Gregory V. Bard

Contact Info

Email bardg@uwstout.edu

Position Associate Professor of Mathematics (since June of 2015)
(was Assistant Professor from August 2011–June 2015; awarded tenure in June of 2016)

Institution The University of Wisconsin—Stout
College of Science, Technology, Engineering, and Mathematics.
Department of Mathematics, Statistics, and Computer Science.

Professional Web Page http://www.uwstout.edu/faculty/bardg/

Personal Web Page http://www.gregorybard.com/

Education

Ph.D.	Applied Math and Scientific Computation	University of Maryland at College Park	Aug 2007
M.Sc.	Applied Math and Scientific Computation	University of Maryland at College Park	Dec 2005
	Visiting Student in Mathematics & History	New College, Oxford University, UK	Spring 2004
M.Sc.	Electrical and Computer Engineering	University of Maryland at College Park	May 2002
B.Sc.	Computer and Systems Engineering, *magna*	Rensselaer Polytechnic Institute	May 1999

Research Interests

- Cryptology, Cryptanalysis, and particularly Algebraic Cryptanalysis
- Computer Algebra (e.g. Solving Polynomial Systems of Equations, and applications of the same)
- Linear Algebra over Finite Fields, with applications in Error Correcting/Detecting Codes
- Operations Research, Optimization, Game Theory, and other applications of Math to Economics
- Security Protocols, Proofs of Security, & Practical Implementations

Previous Employment

Employer	Department	Role	Time
University of Waterloo	Symbolic Comput. Group	Visiting Scholar	6/2012
Fordham University	Mathematics	Visiting Assistant Professor	9/2007 – 5/2011
Chinese Academy of Sciences	Inst. for Math. Mechanization	Visiting Professor	7/2010
Intl. University of Monaco	Doctoral Studies	Visiting Professor	9/2009
University of Maryland	Mathematics	NSF Diss. Completion Fellow	8/2006 – 6/2007
ECRYPT	n/a	Invited Visiting Scientist	5/2006 – 8/2006
American University	Computer Science	Lecturer	1/2005 – 5/2006
University of Maryland	Computer Science	Research Assistant	8/2003 – 4/2004
Naval Surface Warfare Ctr	Active Materials	Summer Intern	5/2003 – 8/2003
University of Maryland	Computer Science	Teaching Assistant	1/2003 – 5/2003
National Security Agency	Research Directorate	Comp. Cryptologic Engineer	5/2001 – 9/2002
National Security Agency	Operations Directorate	Comp. Cryptologic Engineer	6/1999 – 5/2001
National Security Agency	Information Sec. Directorate	Summer Intern	5/1998 – 8/1998
Rensselaer Polytechnic Inst.	Elec. & Comp. Sys. Eng.	Undergraduate Researcher	1/1998 – 5/1998
Rensselaer Polytechnic Inst.	Elec. & Comp. Sys. Eng.	Undergraduate Researcher	1/1997 – 5/1997
Hermes Machine Tool	n/a	Web Developer	5/1996 – 8/1996

Teaching Experience

- This list includes all courses up to and including the Spring 2017 semester.
- The University of Wisconsin—Stout (August 2011 to present)
  - Math-123: Finite & Financial Mathematics (six semesters)
  - Math-153: Calculus I (two semesters)
  - Math-154: Calculus II (seven semesters)
  - Math-270: Discrete Mathematics (five semesters)
  - Math-371: Modern Algebra II (once; independent study for one student)
  - MSCS-380: Cryptography (three semesters)
  - MSCS-747: Scientific Computing (once)
  - CS-480/680: Computer Security (three semesters)
- Fordham University (August 2007 to May 2011)
  - Math-1108: Math for Business: Finite (three semesters)
  - Math-1109: Math for Business: Calculus
  - Math-1204: Applied Calculus II
  - Math-1206: Calculus I (three semesters)
  - Math-1207: Calculus II
  - Math-2004: Multivariate Calculus
  - ‡ Math-2021: Cryptography
  - Math-3002: Differential Equations
  - Math-3005: Abstract Algebra
  - ‡ Math-3021: Graph Theory
  - ‡ Math-4006: Numerical Analysis
  - Math-4999: Bachelor's Thesis and/or Indep. Study (four semesters)
  - The courses marked ‡ were cross-listed with the Computer Science major.
- The Chinese Academy of Sciences—Institute for Mathematics Mechanization (Summer of 2010)
  - Algebraic Cryptanalysis II
- International University of Monaco (October of 2009)
  - Experimental Research, Design, and Assessment
- American University (January 2005 to May 2006)
  - CSC-100: Computers and Information
  - CSC-281: Introduction to Computer Science II
  - CSC-544: Object-Oriented Programming
- University of Maryland at College Park (January 2003 to May 2003)
  - Teaching Assistant for CMSC-858K: Introduction to Cryptography (graduate level)

Publications

Books

In Preparation: G. Bard. *Discrete Structures in Mathematics—A Problem-Solving Perspective.* Roughly 400 out of 800 pages completed.

In Preparation: G. Bard. *Finite & Financial Mathematics.* Roughly 900 out of 1100 pages completed.
`http://www.gregorybard.com/finite.html`

- G. Bard. *Sage for Undergraduates.* The American Mathematical Society. 2015. ISBN: 1-470-41111-3. [Note: 352 pp.]
`http://www.gregorybard.com/books.html`

Note: The American Institute of Mathematics (AIM) placed *Sage for Undergraduates* on its list of "Approved Open-Access Textbooks" judged to meet its strict evaluation criteria. It was the 33rd book to be added to the list. http://aimath.org/textbooks/approved-textbooks/

- G. Bard. *Algebraic Cryptanalysis.* Springer-Verlag. 2009. ISBN: 0-387-88756-3. [Note: 384 pp.]

Patents

Pending: C. Gressel, R. Pinnick, N. Courtois, G. Vago, G. Bard, R. Granot, A. Hecht. *System and Method for Computerized Negotiations Based on Coded Integrity.* Filed July 18, 2013. Published March 13, 2014. Patent Pending. Application No.: US 13 / 945,616.

- C. Gressel, N. Courtois, G. Bard, A. Hecht, R. Granot, T. J. Salmon, I. Mintz. *System and Methods for Encryption with Authentication Integrity.* Filed January 28, 2010. Published August 5, 2010. Awarded October 2, 2012. US Patent No.: 8,280,056.

- C. Gressel, G. Bard, O. Dunkelman, A. Hecht, R. Granot. *System and Method to Preclude Message Modification in Data Authentications Systems through Efficient Use of Feedback in Cryptographic Functions.* Filed Sept 6, 2007. Published March 13, 2008. Awarded October 2, 2012.
US Patent No.: 8,107,622.

Peer-Reviewed Papers

- (For works in progress, see Page 5.)

- Gregory Bard. "An inequality for detecting financial fraud, derived from the Markowitz Optimal Portfolio Theory" Proceedings of the 42nd International Conference on Applications of Mathematics in Engineering and Economics (AMEE'16), Sozopol, Bulgaria. *American Institute of Physics Conference Proceedings*, **Vol. 1789**, No. 1, (V. Pasheva, N. Popivanov and G. Venkov, Eds.), 2016. ISBN: 978-0-7354-1453-2.
`http://www.gregorybard.com/papers/markowitz_fraud_detection_with_appendices.pdf`

- Gregory Bard, Shaun van Ault, and Nicolas Courtois. "Statistics of Random Permutations and the Cryptanalysis Of Periodic Block Ciphers." The journal *Cryptologia.* **Vol. 36** No. 3 (2012), Pp. 240–262, ISSN: 0161-1194.
`http://www.gregorybard.com/papers/courtois_bard_ault.pdf`

- Nicolas Courtois, and Gregory Bard. "Random Permutation Statistics and An Improved Slide-Determine Attack on KeeLoq." *Lecture Notes in Computer Science*, **Vol. 6805**, Pp. 35–54, (David Naccache, Ed.), 2012. ISBN: 3-642-28367-3.
`http://www.gregorybard.com/papers/keeloq_new_paper.pdf`

- Michael Black and Gregory Bard. "SAT Over BOINC: An Application-Independent Volunteer Grid Project." Proceedings of the 12th IEEE/ACM International Conference on Grid Computing (GRID'11), Lyon, France. IEEE Press, Pp 226–227, (Shantenu Jha, Nils Gentschen Felde, Rajkumar Buyya and Gilles Fedak, Eds.), 2011. ISBN: 1-4577-1904-2.
`http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6076480`

- Gregory Bard. "Numerically Estimating Derivatives during Simulations." Proceedings of the 2011 International Conference on Modeling, Simulation, & Visualization Methods (MSV'11). Las Vegas, Nevada. CSREA Press, Pp 341–347, (Hamid Arabnia, Leonidas Deligiannidis, Ashu Solo, and Omer Soysal, Eds.), 2011. ISBN: 1-60132-192-9.
`http://www.gregorybard.com/papers/derivatives.pdf`

- Gregory Bard, Nicolas Courtois, Jorge Nakahara Jr., Pouyan Sepehrdad, and Bingsheng Zhang. "Algebraic, AIDA/Cube and Side Channel Analysis of the KATAN Family of Block Ciphers." Progress in Cryptology (INDOCRYPT'10). Hyderabad, India. *Lecture Notes in Computer Science*, **Vol. 6498**, Pp. 176–196, (Guang Gong and Kishan Chand Gupt, Eds.), 2010. ISBN: 978-3-642-17400-1.
`http://www.gregorybard.com/papers/cube_for_web.pdf`

- Kenneth Wong, and Gregory Bard. "Improved Algebraic Cryptanalysis of QUAD, Bivium, and Trivium via Graph Partitioning on Equation Systems." Proceedings of the Australasian Conference on Information Security and Privacy (ACISP'10). Sydney, Australia. *Lecture Notes in Computer Science*, **Vol. 6168**, Pp. 19–36, (Ron Steinfeld and Philip Hawkes, Eds.), 2010. ISBN: 3-642-14080-7.
`http://eprint.iacr.org/2010/349`

Abstract Only: Gregory Bard. "DEMOCRACY: A Heuristic for Polynomial Systems of Equations over Finite Fields." The journal *ACM Communications in Computer Algebra*. **Vol. 44** No. 1 (2010), Pp. 25–25, ISSN: 1932-2240.
`http://dl.acm.org/citation.cfm?id=1838599.1838613`

Full paper of the above available at:
`http://grim.univ-tln.fr/YACC10/ABSTRACTS/04_bard.pdf`

- Martin Albrecht, Gregory Bard, and Bill Hart. "Algorithm 898: Efficient Multiplication of Dense Matrices over $GF(2)$." *ACM Transactions on Mathematical Software*. **Vol. 37** No. 1 (2009), Pp. 1–14, ISSN: 0098-3500.
`http://www.gregorybard.com/papers/albrecht_bard_hart.pdf`

- Nicolas Courtois, Gregory Bard, and Andrey Bogdanov. "Periodic Ciphers with Small Blocks and Cryptanalysis of KeeLoq." *Tatra Mountains Mathematical Publications*. **Vol. 41** (2008), Pp. 167–188. ISSN: 1210-3195
`http://www.gregorybard.com/papers/keeloq_tatra.pdf`

- Nicolas Courtois, Gregory Bard, and David Wagner, "Algebraic and Slide Attacks on KeeLoq." Proceedings of Fast Software Encryption (FSE'08). Lausanne, Switzerland. *Lecture Notes in Computer Science*, **Vol. 5086**, Pp. 97–115, (K. Nyberg, Ed.), 2008. ISBN 978-3-540-71038-7.
`http://eprint.iacr.org/2007/062`

- Nicolas Courtois and Gregory Bard, "Algebraic Cryptanalysis of the Data Encryption Standard." Proceedings of the IMA International Conference on Cryptography and Coding (IMA-CCC'07). Cirencester, Wales. *Lecture Notes in Computer Science*, **Vol. 4887**, Pp. 152–169, (Steven D. Galbraith, Ed.), 2008. ISBN: 3-540-77271-5.
`http://eprint.iacr.org/2006/402`

- Gregory Bard, "Modes of Encryption Secure Against Blockwise-Adaptive Chosen-Plaintext Attack." Proceedings of the IMA International Conference on Cryptography and Coding (IMA-CCC'07). Cirencester, Wales. *Lecture Notes in Computer Science*, **Vol. 4887**, Pp. 129–151, (Steven D. Galbraith, Ed.), 2008. ISBN: 3-540-77271-5.
`http://eprint.iacr.org/2006/271`

- Gregory Bard, "Spelling-Error and Reordering Tolerant Pass-phrases via the Damerau-Levenshtein String-Edit Distance Metric." Proceedings of the Australasian Information Security Workshop, (AISW'06). Ballarat, Australia. *ACM International Conference Proceeding Series*, **Vol. 249**, Pp. 117–124, (Ljiljana Brankovic, Paul Coddington, John F. Roddick, Chris Steketee, Jim Warren, and Andrew Wendelborn, Eds.), 2007. ISBN: 1-920-68285-X.
`http://eprint.iacr.org/2006/364`

- Gregory Bard, Nicolas Courtois, and Chris Jefferson. "Solution of Sparse Polynomial Systems over GF(2) via SAT-Solvers." Proceedings of the ECRYPT Workshop Tools for Cryptanalysis, (TFC'07). Krakow, Poland. Informally published. (14 pp.), (Jacques Patarin, *et al*, Eds.), 2007.
`http://eprint.iacr.org/2007/024`

- Gregory Bard, "A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL." Proceedings of the IEEE-IACR joint International Conference on Security and Cryptography, (SECRYPT'06). Setúbal, Portugal. Pp. 99–109. (Manu Malek, Eduardo Fernndez-Medina, Javier Hernando, Eds.), 2006. ISBN: 972-8865-63-5.
`http://eprint.iacr.org/2006/136`

- Gregory Bard, "FLOWHUNT— An Attempt at Specification-Based Intrusion Detection using Neural Networks." Proceedings of the 2nd Annual Computer Network Exploitation Conference, (CNE'02). (A conference limited to the US Department of Defense and Intelligence Community, and the Ministries of Defense of certain allied nations, but competitive and peer-reviewed. While the proceedings were classified, this paper, however, was not.) 19 pp.
`http://www.gregorybard.com/papers/flowhunt_for_web.pdf`

Working Papers and Works in Progress

In Preparation: Mark DeBonis and Gregory Bard. "The Interactions between The Veronese Variety and the XL Algorithm of Nicolas Courtois."

In Preparation: Gregory Bard. "On one-time pads that are used twice."

In Preparation: Gregory Bard, and David Hagman. "Are We Lying to Our Children? Conflating Real and Nominal Rates of Return in Saving for Retirement." (11 pp.)

Under Revision: Gregory Bard. "Determining Whether a Given Block Cipher is a Permutation of Another Given Block Cipher (a Problem in Intellectual Property)." (12 pp.)
`http://www.gregorybard.com/papers/bard_permuted_block_cipher.pdf`

Under Revision: Gregory Bard, and Alexander Basyrov. "Error Bounds on Derivatives During Simulations." (11 pp.)
`http://arxiv.org/abs/1212.0280`

Under Revision: Kyle Kloster, and Gregory Bard. "Factoring a semiprime n by estimating $\phi(n)$." This will be a revision of the following Bachelor's Thesis.
`http://www.gregorybard.com/papers/phi_version_may_7.pdf`

Under Revision: Gregory Bard. "New Practical Approximate Matrix Multiplication Algorithms found via Solving a System of Cubic Equations." (17 pp.) A draft has been made available. Some numerical experiments still remain to be done, and will take some time.
`http://www.gregorybard.com/papers/early_release.pdf`

Under Revision: Gregory Bard. "Extending SAT-Solvers to Low Degree Extension Fields of GF(2)." (25 pp.)
`http://www.gregorybard.com/papers/extension_fields.pdf`

Technical Reports and Non-Peer Reviewed Papers

- Martin Albrecht, Gregory Bard, and Clement Pernet. "Efficient Dense Gaussian Elimination over the Finite Field with Two Elements." November 2011. (19 pp.)
  http://arxiv.org/abs/1111.6549
- Nicolas Courtois, Gregory Bard, and Daniel Hulme. "A New General-Purpose Method to Multiply 3×3 Matrices Using Only 23 Multiplications." August 2011. (10 pp.)
  http://arxiv.org/abs/1108.2830
- G. Bard. "DEMOCRACY: A Heuristic for Polynomial Systems of Equations over Finite Fields." October 2010. (7 pp.)
  http://grim.univ-tln.fr/YACC10/ABSTRACTS/04_bard.pdf
- Gregory Bard. "The Application of Polynomials over the Field of Two Elements to a problem in Intellectual Property." (6 pp.)
  http://eprint.iacr.org/2009/326
- Gregory Bard. "Matrix Inversion, LUP-Factorization, and System Solving, via the Method of Four Russians, in $\Theta(n^3/\log n)$ Time." June 2009. (15 pp.)
  http://www.gregorybard.com/papers/m4ri.new.pdf
- K. Wong, G. Bard, and R. Lewis. "Partitioning Multivariate Polynomial Equations via Vertex Separators for Algebraic Cryptanalysis and Mathematical Applications." (33 pp).
  http://www.gregorybard.com/papers/wong_bard_lewis.pdf
- G. Bard, C. Gressel, and A. Hecht. "Security Analysis of the ZK Crypt Data Authenticator and Stream Cipher against Algebraic Cryptanalysis, Differential and Correlation Attacks." This is my security analysis of the ZK-Crypt hash function as part of the NIST competition. (20 pp).
  http://www.gregorybard.com/papers/bard_gressel_hecht.pdf
- G. Bard, "Accelerating Cryptanalysis with the Method of Four Russians." (20 pp).
  http://eprint.iacr.org/2006/251
- G. Bard, "Achieving a log(n) Speed Up for Boolean Matrix Operations and Calculating the Complexity of the Dense Linear Algebra step of Algebraic Stream Cipher Attacks and of Integer Factorization Methods." 20 pp.
  http://eprint.iacr.org/2006/163
- G. Bard. "Algorithms for Fast Matrix Operations." Scholarly paper for Master of Science without Thesis in Applied Mathematics & Scientific Computation, December 2005. 13 pp.
  http://www.gregorybard.com/papers/fast_matrix_operations.pdf
- G. Bard. "Vulnerability of SSL to Chosen-Plaintext Attack." March 2004. 10 pp.
  http://eprint.iacr.org/2004/111

Students & Theses Supervised

- Short summer projects with undergraduates are omitted to save space.
- Joseph Bertino, Mathematics & Economics Double Major at Fordham,
  Bachelor's Thesis defended, May 18, 2011, "Solving Systems of Polynomial Equations Using Gradient Descent and Other Conjugate Gradient Methods, Enhanced by Darwinian and Evolutionary Methods."
  URL Coming Soon!
- Kyle Kloster, Mathematics Undergraduate at Fordham,
  Bachelor's Thesis defended, May 7, 2010. "Factoring a semiprime n by estimating $\phi(n)$."
  http://www.gregorybard.com/papers/phi_version_may_7.pdf

- Michael Levin, Computer Science Master's Candidate at American University,
  Master's Thesis defended, April 22, 2010. "Darwinian Gradient Descent."
  `http://www.gregorybard.com/papers/DarwinianGradientDescent.pdf`

  (Note: I was the director of research and provided career guidance. The nominal supervisor was Prof. Michael Black, then of American University.)

Grants & Funding

- August of 2015. Funded as a consultant to travel to Sammish Island, WA, for "Sage Days 68," to collaborate with some grad students and work on an online appendix to my book *Sage for Undergraduates* about color and 3D-graphing, and other topics not suitable for a black-and-white book.
- Spring of 2015. Invited to address The Fields Institute, as part of the "Workshop on Linear Computer Algebra and Symbolic-Numeric Computation" in October of 2015. All travel expenses, hotel accommodation, and conference fee were paid.
- November of 2014. Awarded a UW Stout "Faculty Fellowship." Named a faculty fellow for 2015. Earned a 3-credit teaching release for the Fall of 2015.
- January of 2015. Received a "Professional Development Grant" from UW Stout to attend the Joint Mathematics Meeting at San Antonio, TX.
- April of 2014. Received a Science, Technology, Engineering, and Math (STEM) College "Small Grant" from UW Stout, to fund three undergraduate researchers in the Summer of 2014.
- January of 2013. Received a "Professional Development Grant" from UW Stout to attend the Joint Mathematics Meeting at San Diego, California.
- December of 2012. Received a "Faculty Research Initiative Major Proposal Development Release" Grant. Teaching release for Fall of 2013 and an undergrad research assistant for Summer of 2013.
- Summer of 2012. Funded as a consultant under two Sage-related NSF grants to travel to Seattle, teach faculty from around the USA how to make interactive web pages in Sage, and attend two Sage-related conferences. (Sage Days 48 and Sage EDU Days 5.) NSF-DUE-1022574. NSF-DMS-1015114.
- Spring of 2012, University of Wisconsin—Stout "Faculty Research Initiative Seed Money" Grant. This is a grant from UW-Stout to fund three undergraduate research assistants to work under my supervision for Summer of 2012. The grant was awarded and all three projects were very successful.
- Academic Year of 2011–2012, awarded a US Department of State "Fulbright Grant" to work with Professor Martin Kreuzer, at the Universität Passau, in Germany, and teach two semester-long classes there. The grant would cover my expenses for travel and living in Germany for one year. Sadly, I had to decline the grant in order to accept my position at the University of Wisconsin—Stout.
- Summer of 2011. Received a "Pi Mu Epsilon Grant" to send three undergrad math-majors (Stephen Fox, Joseph Bertino, and Luigi Patruno) to present their research talks at MathFest.
- This list excludes 5 Fordham University travel grants to conferences, during the period 2007–2011. Also, I had assisted several members of the Fordham Math Department in preparing their own grants.
- Summer of 2010, was invited by the Chinese Academy of Sciences to fly to Beijing and teach 10 classes on Algebraic Cryptanalysis at the Institute for Mathematics Mechanization. Paid for travel and living expenses in China for 5.5 weeks.
- Summer of 2010. Prepared and submitted a "Pi Mu Epsilon Grant" to send two undergraduate math-majors (Alexander Golec and Kyle Kloster) to present their research talks at MathFest.
- Spring of 2010, received support from the National Science Foundation to attend East Coast Computer Algebra Day, in Atlanta, Georgia. They paid for my hotel and airfare.

- Spring of 2009, Fordham Faculty Research Grant. Fordham College of Arts & Sciences funded two undergrad research assistants, for (1) sparse linear algebra over finite fields, and (2) the quadratic sieve.
- Summer of 2008. Prepared and submitted a "Pi Mu Epsilon Grant" to send two undergraduate math-majors (Seena Vali and Daniel DiPasquale) to present their research talks at MathFest.
- Spring of 2008, the Sage project agreed to pay for my flight and hotel to attend a development session at the University of Washington.
- Spring of 2008, Fordham Faculty Research Grant. Fordham College of Arts & Sciences funded an undergrad research assistant, to help set up the *Berkeley Open Interface for Network Computing (BOINC)* on the machines of the campus computer network.
- January of 2008, interdisciplinary seminar support, Fordham University, College of Arts & Sciences. Set up a biweekly seminar in NP-Completeness, between the Math and Computer Science departments.
- November of 2007, the Sage project paid me to attend the "Sage Days 6" conference in Bristol, UK.
- January of 2007, the Sage project paid for my flight and hotel to attend a "coding-sprint" in Los Angeles, California, during which my algorithms would be added to their library.
- Fall of 2006 & Spring 2007, Dissertation Completion Fellowship, NSF VIGRE Program (National Science Foundation, Vertical Integration of Research Program), including full salary plus 10 credits of tuition for one semester.
- Summer of 2006, Visiting Scholar Grant, ECRYPT. The EU's "center of excellence" for the cryptographic community, ECRYPT, funded my living expenses in Paris for the Summer of 2006.
- February of 2006, Travel Grant, NSF VIGRE Program (National Science Foundation, Vertical Integration of Research Program), to fund a trip to Europe to speak at Oxford, to interview for an internship in Paris, and to attend the ECRYPT SASC 2006 Conference in Leuven, Belgium.
- January of 2006, Granted a stipend by the organizers, to attend the "Security Analysis of Stream Ciphers" (SASC'06) conference in Leuven, Belgium.
- Fall 2000 & Spring 2001, National Security Agency's Skills Enhancement Recruitment Incentive Program (SERIP)—Given two semesters of academic leave to pursue a Master's Degree in Electrical & Computer Engineering at the University of Maryland, including full-tuition and full-salary.
- Dean's Scholarship, Rensselaer Polytechnic Institute, 1995, 1996, 1997, 1998.

Service

Referee for Publication

Note: If the list below is surprisingly long, please note that in cryptology it is standard to have 3–5 referees report back on each submission, and so as a result, each researcher is asked to referee rather frequently.

- *25th Conference on Automated Deduction* (CADE'15), refereed 1 paper. Spring 2015.
- *International Conference on Security, Privacy, and Applied Cryptography Engineering* (SPACE'12), refereed 1 paper. Summer 2012.
- The *Cryptographer's Track* of *The RSA Conference* (RSA'11), refereed 1 paper, Fall 2011.
- *The Journal of Mathematical Cryptography*, refereed 1 paper, Spring 2011.
- An advanced textbook for Springer-Verlag, October of 2010.
- *The Journal of Cryptography*, refereed 1 paper, Spring 2010.
- *Integration, the VLSI Journal*, refereed 1 paper, Fall 2009.
- *The Journal of Cryptology*, refereed 1 paper, Summer 2009.

- *Discrete Applied Mathematics*, refereed 1 paper, Summer 2009.
- *ASIACRYPT 2008*, refereed 2 papers, Fall 2008.
- *1st International Conf. on Symbolic Computation and Cryptography.* (SCC'08), refereed 1 paper. Spring 2008.
- *The Journal of Cryptology*, refereed 1 paper, Summer 2007.
- *Applied Cryptography and Network Security.* (ACNS'07), refereed 1 paper. Spring 2007.
- *International Workshop on Coding and Cryptography.* (WCC'07), refereed 1 paper. January 2007.
- *Fast Software Encryption 2007.* (FSE'07), refereed 3 papers. Fall 2006.
- *The 2006 Annual Computer Security Applications Conference.* (ACSAC'06), refereed 3 papers. Fall 2006.
- *Information Security and Cryptology.* (INSCRYPT'06, formerly called CISC), refereed 1 paper. Summer 2006.
- *The 2005 Annual Computer Security Applications Conference.* (ACSAC'05), refereed 4 papers. Fall 2005.

Service to the Profession

- See also, Mathematics Outreach Talks, on Page 13.
- Member of the American Mathematical Society's "Short Course" Committee for the Joint Mathematics Meetings. The committee chooses topics for the 2-day short courses at the JMM. (Fall 2016–present.)
- Trainer for Wisconsin Project Next, sharing with new faculty some software tools useful in teaching 100-level mathematics courses, as part of conferences in Baraboo, Wi (October 13th & 14th, 2012), Marshfield, Wi (April 5th & 6th, 2013), and Baraboo again (November 6th & 7th, 2015).
- Member of a MathFest focus group for the preparation of a calculus text by Michael Sullivan, whose *College Algebra and Trigonometry* textbook is used at UW-Stout. August 2nd, 2012.
- Session Chair for the conference "Modeling, Simulation, and Visualization Methods (MSV'11)," part of the WorldComp 2011 federated conferences. July 20th, 2012.
- Member of a focus group for the preparation of a calculus text by Ray Kunze, aimed at integrating algebra review and detailed examples into the text. January 15th, 2010.
- Session Chair, January 2007 Joint Mathematics Meeting, New Orleans.

Service to the University

- The Faculty Senate:
  - Fall of 2016–Spring 2018, Alternate Faculty Senator, for the Department of Mathematics, Statistics, and Computer Science.
  - Fall of 2016, part of a committee of three to draft the university's "Post-Tenure Review Policy."
  - Fall of 2016, served as Faculty Senate delegate to the UW Stout Library's "Visioning Committee."
  - Fall of 2015, Acting Faculty Senator, covering for a biologist who was on sabbatical.
- From August of 2016 to May of 2017, member of a faculty "Community of Practice" dealing with open-source textbooks and other open/free educational resources for coursework.
- Since March of 2017, member of the advisory board for the "B.Sc. in Retail & Merchandizing Management" program.
- Since May of 2014, member of the advisory board for the "B.Sc. in Business Administration" program.
- Member of the Educational Support Units Review Committee (ESURC) for 2013–14 and 2014–15. This committee investigates units of the university that do not grant degrees (e.g. the library, parking services, the counseling center, Dean of Students office). Each investigation is spearheaded by two members; I took that role that three times, leading the following investigations:

  - Human Resources (Spring 2015).
  - The Office of the Vice-President for Student Life and Services (Fall 2014).
  - The Office of the Dean of the College of STEM (Spring 2014).
- October of 2013, proctored a highly disputed election for the position of chair of the physics department.

- Faculty Representative to the University Website Oversight Committee. (Spring 2012 to Fall 2015.)
  - Assisted in the transition from desktop-only webpages to mobile-friendly and tablet-friendly webpages (a.k.a. "responsive design") for the entire university website infrastructure.
  - In Fall of 2013, spearheaded a campaign to have an undergraduate web designer, funded by federal "work study" program dollars, available to make faculty research webpages out of submitted CVs, as a service to senior faculty members.
  - In May of 2013, helped guide the committee in response to, and recuperation from, a serious hacking incident which vandalized the university web page.

Service to the Department

- At the University of Wisconsin—Stout:
  - Like all members of my department, I have roughly 15 undergrad advisees under my care.
  - Member of the Applied Mathematics & Computer Science Program's Advisory Board since October of 2011.
  - Sole faculty advisor to the club "The Information Security Professionals" since January of 2017.
  - Chairman of the committee to revise our department's Office Hours Policy. (Spring of 2017.)
  - Member of the departmental Curriculum Committee from Fall 2012 to Spring 2016. Read, analyzed, and commented on all new/revised courses from our department. Personally revised
    - MSCS-380/580: *Cryptography*
    - MATH-123: *Finite & Financial Mathematics* (see also, next item)
    - MATH-747: *Scientific Computing*
  - Throughout 2013–2014, organized and co-ordinated a massive reform and revision of MATH-123: *Finite & Financial Mathematics*, working with my department, several program directors, department chairs, and associate deans in the (former) College of Management. Successfully shepherded the course proposal through numerous committees.
  - Member of the Department's Hiring Committee
    - for 2015–16, tenure-track Assistant Professor of Computer Science.
    - for 2014–15, tenure-track Assistant Professor of Computer Science.
    - for 2012–13, tenure-track Assistant Professor of Game Design & Development—Computer Science.
  - Member of the Departmental ad-hoc Committee for the Professional Science Masters Program, since August of 2011.
  - Faculty mentor to new hires.
    - Unofficial faculty mentor to Prof. Jing Xi, 2016–present.
    - Unofficial faculty mentor to Prof. Matt Corne, 2015–present.
    - Official faculty mentor to Prof. Abe Smith, 2015–present.
    - Unofficial faculty mentor to Dr. D. Alex McLaren, 2014–16.
    - Unofficial faculty mentor to Dr. Mark Krines, 2014–15.
    - Official faculty mentor to Dr. David Goluskin, Fall of 2013.
    - Unofficial faculty mentor to Dr. Brian Knaeble, 2012–15.
    - Unofficial faculty mentor to Dr. Nham Ngo, 2012–13.
  - Course coordinator for MATH-154: *Calculus II* for 2014–15, 2015–16, and 2016–17.
  - Course coordinator for MATH-123: *Finite Mathematics* for 2013–14 and 2014–15.
  - Faculty co-advisor for the "Applied Mathematics & Computer Science Club," from August of 2011 to October of 2013.

- Member of the textbook selection committee for
  - MATH-154, *Calculus II*, in Spring 2017.
  - MATH-123, *Finite & Financial Mathematics*, in Fall 2016.
  - CS-480/680, *Computer Security*, in Fall 2015.
  - MSCS-747, *Scientific Computing*, in Fall 2015.
  - MSCS-446, *Numerical Analysis I*, in Spring of 2014.
  - MSCS-380, *Cryptography*, in Spring 2014.
  - MATH-747, *Scientific Computing*, in Fall of 2013.
  - MATH-250, *Differential Equations with Linear Algebra*, in Fall 2012.
  - CS-480, *Computer Security*, in Spring 2012.
- Member of a focus group of faculty who teach CS-courses, to discuss ethics and computer science, for a graduate-student project run by our *Master's in Applied Psychology* program. July 31, 2012.
- Assisted in scoring the ACM International Collegiate Programming Competition, when hosted by UW Stout. (November 5th, 2011.)

- At Fordham University:
  - Supervised two undergraduate honor theses (Spring 2010 and Spring 2011). See "Students Supervised" on Page 6.
  - From Spring 2009 to Spring 2010, also supervised a master's thesis in Computer Science for American University, where I taught previously (Spring 2005–Spring 2006), as a courtesy because that campus did not have a faculty member in the student's desired research topic.
  - Thesis committee for Stephen Fox, an undergraduate honors thesis under the supervision of Prof. Robert Lewis. Spring 2011.
  - Spearheaded an ad-hoc series of training sessions for five undergraduates who wished to take the Mathematics GRE Subject Test, for the purpose of applying to PhD programs. There were five such sessions, four run by me, and one run by a colleague. Fall 2010.
  - Member of the Mathematics Department "Undergraduate Committee" which was redesigning the math-major course requirements. Spring 2009–Fall 2010.
  - Member of a three-person Mathematics Department committee to propose restoring the *Master of Science in Mathematics* degree program, suspended since 1992. Jointly drafted a grant proposal to the NSF for the *Professional Science Masters* program. Fall 2008 to Spring 2010.
  - Chief organizer of an initiative to establish a campus-wide BOINC (Berkeley Open Infrastructure for Network Computing) system to utilize the spare cycles of the computers on the campus. Summer 2008 to Spring 2010.
  - Member of the Fordham Mathematics Department, Committee on Math Methods in Business preparation and assessment. Spring 2008.
  - In reference to above, co-authored the "Calculus Readiness Examination," thirty very short questions to test basic math skills for calculus students in the business school. Spring 2008.
  - Created "The Remedial Math Reserve," a collection of 8 outstanding remedial texts for students struggling with calculus. One set of each went to the "Math Help Room" and the Fordham University library. Spring 2008.
  - Faculty Co-Advisor of Pi Mu Epsilon, the undergraduate mathematics honor society. Spring 2008 to Fall 2010.
  - Member of the Gay, Lesbian, Bisexual, Questioning and Allies "Campus Climate Committee," a collection of faculty, students, Jesuits, residence associates, and staff. Academic year 2007–08.
  - Faculty Co-Advisor of the Fordham Math Club. Academic year 2007–2008.

- During graduate school at the University of Maryland at College Park:
  - Judge, Fall 2006 Spotlight on Graduate Research, Oral Presentation Contest.
  - Graduate Student Mentor—was assigned a first-year graduate student to guide and mentor through the Applied Mathematics PhD program, Fall 2006 to Spring 2007.
  - Coach, American University's "Alpha Team" for the ACM International Collegiate Programming Competition — Trained, coached, organized and prepared three undergraduates (two from computer science and one from mathematics) for the five-hour annual ACM programming contest. Team placed 53rd out of 154 teams in the Mid-Atlantic Region. (Fall 2005.)
  - Judge, Fall 2005 Spotlight on Graduate Research, Oral Presentation Contest.
- During my undergraduate years at Rensselaer Polytechnic Institute (RPI):
  - Founder & President, Rensselaer Cryptographic Club, Fall 1998 to Spring 1999.
  - Member, Dean's Advisory Commission for the School of Engineering, 1997–98, and 1998–99.
  - Member, President's Advisory Council on Diversity. 1995–96 and 1996–97.

Community Service

- Wisconsin Science Olympiad (WSO). Since April of 2013, I have run the "Codes & Algorithms" event called "Code Busters." This includes making a website, posting rules, designing questions and answers. I also made a series of online interactive webpages to help students prepare. I write the exams for the state-level event, and the Boyceville Invitational event at Boyceville High School.
- National Science Olympiad (NSO). In May of 2016, I ran the "Code Busters" event at the national level, which had never been done before.
- Elections Judge, 2^{nd} Precinct, 14^{th} District, State of Maryland. Setup and closed the polling place, trained volunteers, assisted the blind and deaf, adjudicated exceptions, counted ballots, certified the process. A paid position with a training course and an oath of office. (Primary Election and General Election of 2006). Counted 709 and 1821 ballots respectively.
- See also, Mathematical Outreach Talks, below.

Mathematical Outreach Talks

1. Festival of Scientific Computing, University of Wisconsin—Stout. March 3rd, 2017. "A New Application of the Markowitz Optimal Portfolio Theory and Its Efficient Frontier: Detecting Investment Fraud (e.g. Ponzi Schemes)."
2. STEM Career Day, University of Wisconsin—Stout. October 24th, 2014. (Talk given twice in the same day.) "Mathematics and Cracking Secret Codes."
3. Wisconsin Science Olympiad—Coaches' Clinic. University of Wisconsin—Stout. April 13, 2014. "Preparing Students for the 'Code Busters' Event."
4. STEM Career Day, University of Wisconsin—Stout. November 1, 2013. (Talk given twice in the same day.) "Mathematics and Cracking Secret Codes."
5. IEEE Student Chapter, University of Wisconsin—Stout. April 17, 2013. "Breaking Codes by Solving Polynomials: Algebraic Cryptanalysis."
6. AMCS Club Putnam Team, University of Wisconsin—Stout. November 28, 2012. "Integer Solutions to Matrix Problems."
7. STEM Career Day, University of Wisconsin—Stout. November 2, 2012. (Talk given twice in the same day.) "Mathematics and Cracking Secret Codes."

8. Applied Science Speaker Series. University of Wisconsin—Stout. September 27, 2012. "Sage and Regressions in Science."

9. AMCS Club Putnam Team, University of Wisconsin—Stout. November 30, 2011. "Diophantine Matrix Problems and the Archimedes Bovine Problem."

10. Public Lecture, Fordham University, New York. May 6, 2011. "Babylonian Mathematics."

11. Math Club, Fordham University, New York. February 3, 2011. "Vandermonde, Sequences, Wittgenstein, and Sage."

12. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, New Orleans, Louisiana. January 8, 2011. "Exploring Game Theory with Sage, the open-source competitor to Maple, Mathematica, Matlab and MAGMA."

13. Science Club, Iona College, New York. October 22, 2009. "My Experiences at the NSA."

14. REU in Cryptanalysis, Northern Kentucky University. August 4, 2009. "Partitioning Multivariate Polynomial Systems of Equations via Vertex Cuts."

15. Math Club, Fordham University, New York. November 12, 2008. "Mathematics on Clay Tablets."

16. Math Club, Iona College, New York. November 5, 2008. "Strange Notions of Distance and Error-Correcting Passwords."

17. Center for Talented Youth Visit to Fordham University, New York. April 12, 2008. "Unlocking the Puzzle: A Survey of how Polynomial Systems of Equations are used to solve problems in Medical Imaging, Information Security, Aerodynamics, The Search for Extraterrestrial Intelligence (SETI), and Rational Drug Design."

18. Math Club, Iona College, New York. November 8, 2007. "What is Chaos Theory?"

19. Math Club, Fordham University, New York. October 3, 2007. "Algebraic Cryptanalysis."

20. Mathematics Book Club, University of Maryland. April 25, 2006. "Using Matrices to Break Modern Satellite and Telephony Codes."

21. Lecture Series, The Historical Miniatures Gaming Society, Gettysburg, Pennsylvania. November 11 & 12, 2005. "What is Game Theory?"

22. School of Computer, Mathematical and Physical Sciences, University of Maryland. October 21, 2005. "Science & Technology: Addressing the Need for Diversity (STAND) 'Math Exploration Day' talk on Cæsar Ciphers and Secret Decoder Rings."

23. Oxford Computing Society, May 25, 2004, "The Vulnerability of SSL to Chosen-Plaintext Attack."

Honors & Awards

- UW Stout "Faculty Research Fellow" for 2017–2018.
- UW Stout "Faculty Research Fellow" for 2015–2016.
- "Certificate of Achievement," Assoc. for Computing Machinery, for leading the American University 2005 Programming Team to an "Honorable Mention" in the Mid-Atlantic Conference (Nov. 2005).
- Winner, 2004–2005 "Spotlight on Graduate Research" Award, Department of Mathematics, University of Maryland, for my work on building hash-function families from pseudorandom function families. There were four total winners from among the Pure Math, Applied Math, Scientific Computation and Statistics programs. Included a cash award. (Nov. 2005).

- Ranked first place out of 21 Pure & Applied Mathematics students in the algebra written Qualifying Exams for the PhD program. (August 2005).
- Registered "Visiting Advanced Student," Oxford University, New College, 2004.
- NSA Eagle Award, December 1999, 2000, 2001, for charitable & community service acts.
- While at the NSA, seven letters of commendation and The Director's Star Award, August 1998, Note, two letters were signed by Michael Hayden, at that time a 3-star general and Director of the NSA.
- National Merit Scholarship Semi-Finalist, June 1995.

Invited Talks & Presentations

(sched.) The Mathematical Association of America MathFest Conference, Chicago, IL. July 28th, 2017. "Realistic Examples of Bayes's Rule from Cybersecurity."

(sched.) The 7th International Conference on Algebraic Informatics (CAI'17) Cryptography and Coding Theory Track, Kalamata, Greece. June 28th, 2017. "Determining Whether a Given Block Cipher is a Permutation of Another Given Block Cipher (a Problem in Intellectual Property)."

(sched.) The 43rd International Conference on Applications of Mathematics in Engineering and Economics (AMEE'17), Sozopol, Bulgaria. June 9th, 2017. "Bayesian Reasoning in Computer Science and Cybersecurity."

1. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, Atlanta, GA. January 7th, 2017. "Four Problems from Computing to Enhance Student Enthusiasm in the Discrete Mathematics Classroom."
2. The Mathematical Association of America MathFest Conference, Columbus, OH. August 4th, 2016. "A New Application of the Markowitz Optimal Portfolio Theory and Its Efficient Frontier."
3. The 42nd International Conference on Applications of Mathematics in Engineering and Economics (AMEE'16), Sozopol, Bulgaria. June 12th, 2016. "A New Application of the Markowitz Optimal Portfolio Theory and its Efficient Frontier."
4. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, Seattle, WA. January 8th, 2016. "The Two-Time Pad Problem: Plaintext Recovery for One-Time Pads Used Twice."
5. Wisconsin Project NEXT, Fall Meeting. Baraboo, Wisconsin. November 7th, 2015. "The Two-Time Pad Problem: Examined from the Teaching, Scholarship, and Service Perspectives."
6. The Fields Institute, Workshop on Linear Computer Algebra and Symbolic-Numeric Computation, Toronto, Ontario. October 28th, 2015. "Exploring the Extended Linearization Algorithm (or XL Algorithm) for Solving Polynomial Systems of Equations, with Remarks toward NP-Completeness."
7. Departmental Seminar. University of Wisconsin—Stout. October 2nd, 2015. "Introducing SageMathCloud."
8. The Applications of Computer Algebra Conference (ACA'15), Kalamata, Greece. July 20th, 2015. "Using SageMathCell and Sage Interacts to Reach Mathematically Weak Business Students."
9. The Applications of Computer Algebra Conference (ACA'15), Kalamata, Greece. July 23rd, 2015. "A Brief Introduction to the Extended Linearization Method (or XL Algorithm) for Solving Polynomial Systems of Equations."
10. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, San Antonio, TX. January 12th, 2015. "Computing the Least Factorial that Multiplies a Rational Number into an Integer."

11. The Mathematical Association of America MathFest Conference, Portland, Oregon. August 7th, 2014. "Macroeconomics in Finite Math: Rediscovering and Recreating Leontief Analysis."

12. The Applications of Computer Algebra Conference (ACA'14), Fordham University, The Bronx, NY. July 11th, 2014. "Plaintext Recovery for One-Time Pads that are Used Twice."

13. Departmental Colloquium, University of Minnesota—Duluth. May 1st, 2014. "What is Algebraic Cryptanalysis?"

14. Departmental Colloquium, University of Wisconsin—River Falls. April 22nd, 2014. "Breaking Codes by Solving Polynomials: Algebraic Cryptanalysis."

15. Southeastern Regional Meeting of the American Mathematical Society (AMS) Louisville, Kentucky. October 5th, 2013. "Reducing the Number of Variables in a System of Equations during Algebraic Cryptanalysis, by Constructing a Forest."

16. Departmental Seminar. University of Wisconsin—Stout. September 13th, 2013. "A Demo of The Sage Single-Cell Server, SageMathCloud, and Sage Applets."

17. The 7th Annual Best Practices in STEM Conference, Baraboo, Wisconsin. August 21st, 2013. "Use of Interactive Webpages in Teaching."

18. Sage Education Days V, Seattle, Washington, June 21st, 2013. "Using Sage while Teaching Financial Math (and Calculus Too!)"

19. The 6th Annual Polytechnic Summit, Boston, Massachusetts. June 6th, 2013. "Rethinking Finite Math: Bridging Boundaries between Mathematics, Economics, Finance, and Business."

20. The Mathematical Association of America (MAA) Wisconsin Sectional Meeting, Marshfield, Wisconsin. April 5th, 2013. "Emerging Technologies in Mathematics Instruction."

21. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, San Diego, California. January 12, 2013. "Pivoting Strategies in Sparse Gaussian Eliminations done mod p and their Impact upon Various Computer Algebra Tasks."

22. Wisconsin Project NEXT, Fall Meeting. Baraboo, Wisconsin. October 14, 2012. "Sage for the College Math Professor."

23. The 6th Annual Best Practices in Science, Math and Engineering Teaching Conference. Baraboo, Wisconsin. August 23, 2012. "Using Sage in Lower-Division Undergraduate Science Courses to Explore Functions, their Graphs, and Regressions."

24. SIAM Annual Meeting 2012. Minneapolis, Minnesota. July 9, 2012. "Breaking Codes by Solving Polynomials: Algebraic Cryptanalysis!"

25. Symbolic Computation Group Seminar. University of Waterloo, Ontario. June 13, 2012. "Breaking Codes by Solving Polynomials: Algebraic Cryptanalysis."

26. EUROCRYPT'12, Cambridge, United Kingdom. April 17, 2012. Rump-Session Talk: "A Professional Science Masters in Applied Mathematics."

27. College of Science, Technology, Engineering and Mathematics Short Talks. University of Wisconsin, Stout. December 2, 2011. "Algebraic Cryptanalysis: The Science of Breaking Codes with Polynomials."

28. Departmental Colloquium. University of Wisconsin, Stout. October 14, 2011. "Exploring Sage in Calculus, Linear Algebra, College Algebra, and Differential Equations."

29. SIAM Conference on Applied Algebraic Geometry (AG'11). Raleigh, North Carolina. October 7, 2011. "Pivoting Strategies for Sparse Matrices over Finite Fields."

30. Modeling, Simulation, and Visualization Methods (MSV'11). Las Vegas, Nevada. July 21, 2011. "Numerically Estimating Derivatives during Simulations."

31. The 10th International Conference on Finite Fields and their Applications (Fq'10). Ghent, Belgium. July 12, 2011. "The Nucleus-Cloud Method for Simplifying Polynomial Systems mod 2."

32. The Cryptography Group, The Graduate Center of the City University of New York. April 8, 2011. "Fixed Points, and Algebraic Cryptanalysis."

33. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, New Orleans, Louisiana. January 9, 2011. "DEMOCRACY: a new technique for solving polynomial systems of equations over finite fields via stochastic local search."

34. Discrete Mathematics Seminar, Columbia University, New York. November 9, 2010. "A new technique for solving polynomial systems of equations over finite fields via stochastic local search."

35. The Cryptography Group, The Graduate Center of the City University of New York. October 29, 2010. "Solving Under-defined Polynomial Systems over Finite Fields."

36. YACC'10. Porquerolles Island, near Toulon, France. October 6, 2010. "DEMOCRACY—A Heuristic for Polynomial Systems of Equations over Finite Fields."

37. East Coast Computer Algebra Day (ECCAD'10). Emory University, Georgia. May 15, 2010. "Democracy: An Iterative Approximation Heuristic for Solving Polynomial Systems of Equations mod Small Odd Primes using the Greedy Algorithm."

38. Workshop on Mathematics of Post-Quantum Cryptography. Stevens Institute of Technology, New Jersey. March 27, 2010. "Using Graph Theory to Split Polynomial Systems of Equations."

39. The Cryptography Group, The Graduate Center of the City University of New York. February 19, 2010. "SAT-solvers and Algebraic Cryptanalysis."

40. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, San Francisco, California. January 13, 2010. "Algebraic Attacks on Bivium and Trivium, Accelerated by Cutting the Variable-Sharing Graph."

41. Department of Mathematics and Computer Science, Seton Hall, New Jersey. October 9, 2009. "Partitioning Multivariate Polynomial Equations via Vertex Cuts."

42. Applications of Computer Algebra (ACA'09), Montreal, Quebec. June 28, 2009. "Partitioning Multivariate Polynomial Equations via Vertex Cuts."

43. EUROCRYPT'09, Cologne, Germany. April 28, 2009. Rump-Session Talk: "Distinguishing Attacks on Highly-Iterated Ciphers."

44. Discrete Mathematics Seminar, Columbia University, New York. February 10, 2009. "Exponential Generating Functions, High Powers of Random Permutations, and Very Iterated Block Ciphers."

45. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, Washington, DC, USA. January 8, 2009. "Ultra-Sparse Matrix Reduction to Reduced Row-Echelon Form for matrices over $GF(2)$."

46. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, Washington, DC, USA. January 8, 2009. "Solving an Intellectual Property Problem via A System of Polynomial Equations over $GF(2)$."

47. Mathematics Department Colloquium Talks. United States Naval Academy. October 29, 2008. "Using Graph Theory to Control Fill-in for Sparse Matrix Reduction to RREF over Fields of non-Zero Characteristic."

48. Sage Days 10. Nancy, Lorraine, France. October 10, 2008. "Using Graph Theory to Control Fill-in for Sparse Matrix Reduction to RREF over Fields of non-Zero Characteristic."

49. Central European Conference on Cryptography. Graz, Austria. July 2, 2008. "Extending SAT-Solvers to Low Degree Extension Fields of GF(2)."

50. Theory Reading Group. Columbia University, New York. February 27, 2008. "On the Vertex-Connection Number of a particular graph of of a Polynomial System of Equations over a Finite Field."

51. University of Maryland Mathematics Department Algebra Colloquium, February 25, 2008. "Matrix Multiplication in time $n^{2.777}$."

52. IMA International Conference on Cryptography and Coding. Cirencester, UK. December 18, 2007. "Modes of Encryption Secure Against Blockwise-Adaptive Chosen-Plaintext Attack."

53. Sage Days 6, Bristol, UK. November 12, 2007. "A Plea for Help: Progress on a Practical Algorithm for Massively-Parallel Dense Matrix Multiplication in time $n^{2.777}$ over any Field someday, but for now, the Reals."

54. ECRYPT Tools for Cryptanalysis Special Workshop. Krakow, Poland. September 25, 2007. "Solution of Sparse Polynomial Systems over $GF(2)$ via SAT-Solvers."

55. The 8th International Conference on Finite Fields. Melbourne, Australia. July 11, 2007. "On the Connection Number of a Particular Graph of a Polynomial System of Equations over a Finite Field."

56. The 7th Central European Conference on Cryptology. Smolenice, Slovakia. June 22, 2007. "Building a Trap-Door One-Way Function from a Multivariate Quadratic System of Equations."

57. University of Maryland Mathematics Department Graduation Conference, April 13, 2007, "Inverting Dense Boolean Matrices in Faster than Cubic Time."

58. Sage Days 3. University of California at Los Angeles, Institute for Pure and Applied Mathematics, February 17, 2007. "The Method of Four Russians."

59. University of Wollongong, New South Wales, Australia, February 8, 2007. "Solving Systems of Polynomial Equations over GF(2), and its Applications to Cryptanalysis."

60. Australasian Information Security Workshop. Ballarat, Australia. January 31, 2007. "Spelling-Error and Reordering Tolerant Pass-phrases via the Damerau-Levenshtein String-Edit Distance Metric."

61. Royal Holloway, University of London. January 23, 2007. "Solving a System of Polynomial Equations with a SAT-Solver."

62. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, New Orleans, USA. January 5, 2007. "Algorithms for Inverting or LUP-Factoring Matrices over $GF(2)$ in time $O(n^3/\log n)$."

63. Applied Mathematics Research Interaction Team for Cryptology, University of Maryland, September 27, 2006, "SAT Solvers and Polynomials."

64. Royal Holloway, University of London. August 15, 2006. "A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack."

65. SECRYPT'06, Setúbal, Portugal. August 8, 2006. "A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL."

66. Ecole Nationale Supérieure de Techniques Avancées (ENSTA). July 7, 2006. "Boolean Matrix Operations." (Invited Seminar talk as part of their research group's weekly series).

67. Université de Versailles Saint-Quentin-en-Yvelines. June 28, 2006. "Matrix Operations and Boolean Algebra." (Invited Seminar talk as part of their research group's weekly series).

68. YACC'06, Porquerolles Island, near Toulon, France. June 19, 2006. "Modes of Encryption Secure against Blockwise-Adaptive Chosen-Plaintext Attack."

69. EUROCRYPT'06, St. Petersburg, Russia. May 30, 2006. Rump-Session Talk: "Using the Method of Four Russians for Dense Boolean Matrix Inversion."

70. Applied Mathematics Research Interaction Team for Cryptology, University of Maryland, April 24, 2006, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics or Other Noisy Data."

71. Special Seminar, Computing Laboratory, Oxford University. January 31, 2006, "Boolean matrices, cryptography and constraint satisfaction."

72. Applied Mathematics Research Interaction Team for Cryptology, University of Maryland, September 26, 2005, "Matrices over GF(2) and Stream Cipher Cryptanalysis, an Introduction."

73. "Spotlight on Graduate Research" Competition Victory Presentation, University of Maryland, May 4, 2005, "Building Cryptographic Hash Functions from Pseudorandom Function Families."

74. Applied Mathematics Research Interaction Team for Cryptology, University of Maryland, April 20, 2005, "Pseudorandom Function Domain Extension Using Directed Acyclic Graphs."

75. Oxford Computing Laboratory, Security & Concurrency Research Group, June 23, 2004, "Four Particular Open Questions in Cryptography."

76. Applied Mathematics Research Interaction Team for Cryptology, University of Maryland, March 2, 2005, "Black-Box Analysis of the Block-Cipher Based Hash Function Constructions from PGV."

77. "Spotlight on Graduate Research" Competition Entry, November 22, 2004, "Building Scalable Almost-XOR Universal Hash Functions from Pseudorandom Function Families."

78. Applied Mathematics Research Interaction Team for Cryptology, University of Maryland, Sept 22 & 29, 2004. "Online Encryption Schemes resistant to Blockwise Adaptive Chosen Plaintext Attack."

79. Applied Mathematics Research Interaction Team for Cryptology, University of Maryland, March 10, 2004. "Solving Systems of Polynomial Equations in GF(2)."

80. Applied Mathematics Research Interaction Team for Cryptology, University of Maryland, September 17, 2003. "Cryptanalysis of Non-Linear Stream Ciphers using Very Large Matrices."

81. Department of Computer Science, Cryptology Reading Group, University of Maryland, February 14, 2003. "Blockwise-Adaptive Security."

82. Department of Computer Science, Cryptology Reading Group, University of Maryland, October 29, 2002. "The Security of SSH."

83. Second Annual Computer Network Exploitation Conference, Spring 2002, "FLOWHUNT—An attempt at Specification-Based Intrusion Detection."