Gregory V Bard

Associate Professor, University of Wisconsin-Stout
Mathematics, Statistics & Computer Science Department
College of Science, Technology, Engineering, Mathematics and Management

Office: 225 Jarvis Hall-Science Wing
Phone: 715-232-1357
Email: bardg@uwstout.edu

Research Interests: Cryptology, and particularly Algebraic Cryptanalysis. 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.

Education

- **Ph D Applied Math and Scientific Computation**
  University of Maryland at College Park
  College Park, MD, 2007
- **MS Applied Math and Scientific Computation**
  University of Maryland at College Park
  College Park, MD, 2005
- **MS Electrical and Computer Engineering**
  University of Maryland at College Park
  College Park, MD, 2002
- **BS Computer and Systems Engineering**
  Rensselaer Polytechnic Institute
  1999

Work Experience

Academic - Post-Secondary

- **University of Wisconsin-Stout**, Mathematics, Statistics and Computer Science Department
  Associate Professor
  July 2016 -
- **University of Wisconsin-Stout**, Mathematics, Statistics and Computer Science Department
  Assistant Professor
  August 2011 - June 2016
- **Fordham University**, Mathematics
  Visiting Assistant Professor
  2007 - 2011
- **Chinese Academy of Sciences**, Inst. for Math. Mechanization
  Visiting Professor
  2010 - 2010
- **InternationaUniversity of Monaco**, Doctoral Studies
  Visiting Professor
  October 2009 - October 2009
- **American University**, Computer Science
  Lecturer
  2005 - 2006

- **University of Maryland**, Computer Science
  Research Assistant
  Present
- **University of Maryland**, Computer Science
  Teaching Assistant
  Present

Intellectual Contributions

Book

- Bard, G. V. (In Preparation; Not Yet Submitted). Finite & Financial Mathematics for University Freshmen. , Atlantis Publications.
- Bard, G. V. Sage for Undergraduates. , 352, The American Mathematical Society.
- Bard, G. V. Algebraic Cryptanalysis. *, 384*, Springer-Verlag.

Presentations

Uncategorized

- Bard, G. V. (January 12, 2015). Computing the Least Factorial that Multiplies. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, San Antonio, TX.
- Bard, G. V. (August 7, 2014). Macroeconomics in Finite Math: Rediscovering and Recreating Leontief Analysis. The Mathematical Association of America MathFest Conference, Portland, OR.
- Bard, G. V. (July 11, 2014). Plaintext Recovery for One-Time Pads that are Used Twice. The Applied Computer Algebra Conference, The Bronx, NY.
- Bard, G. V. (May 1, 2014). What is Algebraic Cryptanalysis?. Departmental Colloquium, Dutluth, MN.
- Bard, G. V. (April 22, 2014). Breaking Codes by Solving Polynomials: Algebraic Cryptanalysis. Departmental Colloquium, River Falls, WI.
- Bard, G. V. (October 5, 2013). Reducing the Number of Variables in a System of Equations during Algebraic Cryptanalysis, by Constructing a Forest. Southeastern Regional Meeting of the American Mathematical Society (AMS), Louisville, KY.
- Bard, G. V. (September 13, 2013). A Demo of The Sage Single-Cell Server, SageMathCloud, and Sage Applets. Departmental Seminar, Menomonie, WI.
- Bard, G. V. (August 21, 2013). Use of Interactive Webpages in Teaching. The 7th Annual Best Practices in STEM Conference, Baraboo, WI.
- Bard, G. V. (June 21, 2013). Using Sage while Teaching Financial Math (and Calculus Too!). Sage Education Days V, Seattle, WA.
- Bard, G. V. (June 6, 2013). Rethinking Finite Math: Bridging Boundaries between Mathematics, Economics, Finance, and Business. The 6th Annual Polytechnic Summit, Boston, MA.
- Bard, G. V. (April 5, 2013). Emerging Technologies in Mathematics Instruction. The Mathematical Association of America (MAA) Wisconsin Sectional Meeting, Marshfield, WI.
- Bard, G. V. (January 12, 2013). Pivoting Strategies in Sparse Gaussian Eliminations done mod p and their Impact upon Various Computer Algebra Tasks. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, San Diego, CA.
- Bard, G. V. (October 14, 2012). SAGE for the College Math Professor. Wisconsin Project NEXT, Fall Meeting, Baraboo, WI.
- Bard, G. V. (August 23, 2012). Using SAGE in Lower-Division Undergraduate Science Courses to Explore Functions, their Graphs, and Regressions. The 6th Annual Best Practices in Science, Math and Engineering Teaching Conference, Baraboo, WI.
- Bard, G. V. (July 9, 2012). Breaking Codes by Solving Polynomials: Algebraic Cryptanalysis!. SIAM Annual Meeting 2012, Minneapolis, MN.
- Bard, G. V. (June 13, 2012). Breaking Codes by Solving Polynomials: Algebraic Cryptanalysis. Symbolic Computation Group Seminar, Waterloo, Ontario.

- Bard, G. V. (April 17, 2012). A Professional Science Masters in Applied Mathematics. EUROCRYPT'12, Cambridge, United Kingdom.
- Bard, G. V. (December 2, 2011). Algebraic Cryptanalysis: The Science of Breaking Codes with Polynomials. College of Science, Technology, Engineering and Mathematics Short Talks, Menomonie, WI.
- Bard, G. V. (October 14, 2011). Exploring SAGE in Calculus, Linear Algebra, College Algebra, and Dierential Equations. Departmental Colloquium, Menomonie, WI.
- Bard, G. V. (October 7, 2011). Pivoting Strategies for Sparse Matrices over Finite Fields. SIAM Conference on Applied Algebraic Geometry (AG'11), Raleigh, NC.
- Bard, G. V. (July 21, 2011). Numerically Estimating Derivatives during Simulations. Modeling, Simulation, and Visualization Methods (MSV'11), Las Vegas, NV.
- Bard, G. V. (July 12, 2011). The Nucleus-Cloud Method for Simplifying Polynomial Systems mod 2. The 10th International Conference on Finite Fields and their Applications (Fq'10), Ghent, Belgium.
- Bard, G. V. (April 8, 2011). Fixed Points, and Algebraic Cryptanalysis. The Cryptography Group, New York City, NY.
- Bard, G. V. (February 23, 2011). Multivariate Polynomial Systems. Department of Math., Stat., and Comp. Sci.,, Menomonie, WI.
- Bard, G. V. (January 9, 2011). DEMOCRACY: a new technique for solving polynomial systems of equations over nite elds via stochastic local search. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, New Orleans, LA.
- Bard, G. V. (December 3, 2010). Polynomials in Characteristic 2 and Logical Satisability: The Connections between Algebraic Cryptanalysis and SAT-Solvers. Department of Mathematics, Fort Myers, FL.
- Bard, G. V. (November 9, 2010). A new technique for solving polynomial systems of equations over nite elds via stochastic local search. Discrete Mathematics Seminar, New York, NY.
- Bard, G. V. (October 29, 2010). Solving Under-dened Polynomial Systems over Finite Fields. The Cryptography Group, New York, NY.
- Bard, G. V. (October 6, 2010). DEMOCRACY-A Heuristic for Polynomial Systems of Equations over Finite Fields. YACC'10, Porquerolles Island, France.
- Bard, G. V. (May 15, 2010). Democracy: An Iterative Approximation Heuristic for Solving Polynomial Systems of Equations mod Small Odd Primes using the Greedy Algorithm. East Coast Computer Algebra Day (ECCAD'10), Atlanta, GA.
- Bard, G. V. (March 27, 2010). Using Graph Theory to Split Polynomial Systems of Equations. Workshop on Mathematics of Post-Quantum Cryptography, Hoboken, NJ.
- Bard, G. V. (March 11, 2010). Algebraic Cryptanalysis and Polynomial Systems of Equations. Department of Mathematics, New York, NY.
- Bard, G. V. (February 19, 2010). SAT-solvers and Algebraic Cryptanalysis. The Cryptography Group, New York, NY.
- Bard, G. V. (January 29, 2010). The Inverse Trigonometric Functions and their Derivatives, with Applications to Integration. Department of Mathematics and Computer Science, Atlanta, GA.
- Bard, G. V. (January 13, 2010). Algebraic Attacks on Bivium and Trivium, Accelerated by Cutting the Variable-Sharing Graph. Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Metting, San Francisco, CA.
- Bard, G. V. (October 9, 2009). Partitioning Multivariate Polynomial Equations via Vertex Cuts. Department of Mathematics and Computer Science, South Orange, NJ.
- Bard, G. V. (June 28, 2009). Partitioning Multivariate Polynomial Equations via Vertex Cuts. Applications of Computer Algebra (ACA'09), Montreal, Quebec, Canada.
- Bard, G. V. (April 28, 2009). Distinguishing Attacks on Highly-Iterated Ciphers. EUROCRYPT'09, Cologne, Germany.
- Bard, G. V. (March 13, 2009). Using polynomials to break block ciphers. Department of Mathematics, Rochester, NY.
- Bard, G. V. (March 3, 2009). Cryptanalytic Adventures, in Polynomial and Linear Systems of Equations, mod 2. Department of Mathematics, Philadelphia, PA.

- Bard, G. V. (February 13, 2009). The Algebraic Cryptanalysis of KeeLoq. Department of Mathematics, New Orleans, LA.
- Bard, G. V. (February 10, 2009). Exponential Generating Functions, High Powers of Random Permutations, and Very Iterated Block Ciphers. Discrete Mathematics Seminar, New York, NY.
- Bard, G. V. (January 8, 2009). Solving an Intellectual Property Problem via A System of Polynomial Equations over GF(2). Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, DC.
- Bard, G. V. (January 8, 2009). Ultra-Sparse Matrix Reduction to Reduced Row-Echelon Form for matrices over GF(2). Mathematical Association of America (MAA) and American Mathematical Society (AMS) Joint Mathematics Meeting, DC.

Grants, Contracts, and Sponsored Research

Grant

- Stricker, D., Bard, G. V., Bomar, C., Lee, S. A., & Schultz, F. S. 2014) STEM Education in a Digital World: Apps in the Classroom, a Wisconsin Improving Teacher Quality grant.