# Curriculum Vitae of Christopher Monico

Department of Mathematics and Statistics
Texas Tech University
Lubbock, TX 79409-1042
email: c.monico@ttu.edu
March 10, 2016

## Positions held

| | |
|---|---|
| 2009–present | Associate Professor, Texas Tech University. |
| 2003–2009 | Assistant Professor, Texas Tech University. |
| 2002–2003 | Postdoctoral Researcher, University of Notre Dame. |
| 2001–2002 | Fellowship from the Center of Applied Mathematics, University of Notre Dame. |
| 1998–2001 | Teaching Assistantship, University of Notre Dame. |
| 1996–1997 | |
| 1997–1998 | Systems Analyst/Programmer, Ilex Systems / $L^3$ Communications, Shrewsbury, NJ. |

## Education

| | |
|---|---|
| 2002 | Ph.D in Mathematics, University of Notre Dame. Dissertation: "Semirings and semigroup actions in public-key cryptography". Advisor : Joachim Rosenthal |
| 2000 | M.S. in Mathematics, University of Notre Dame. |
| 1996 | B.S. in Mathematics, Computer Science minor, Monmouth University. |

## Research Interests

I have worked on computational problems in general, and specifically discrete computational problems, such as the discrete logarithm problem and zero-dimensional primary decomposition. This work has included trying to build efficient cryptosystems on the semigroup action problem, and using distributed computing to solve large problems (i.e., Certicom's *ECCp-109 challenge*). I am also interested in integer factorization; my `GGNFS` number field sieve software (distributed with Jens Franke's lattice siever) has been used by many people worldwide to factor large integers as part of various projects.

I am also interested in some general algebraic and number theoretic problems motivated by cryptographic concerns. In my dissertation, I classified finite, non-idempotent, additively commutative simple semirings. I also gave an algorithm for computing the primary decomposition of zero-dimensional ideals. More recently, I have become interested in additive (combinatorial) structure on the fibers of characters on $\mathbb{F}_p^*$ for possible use in studying the distribution of quadratic non-residues.

## Publications

**(1)** C. Monico. "Cryptanalysis of a matrix-based MOR system." *Comm. Algebra*, 44 (2016), pp. 218–227.

**(2)** C. Monico, M. D. Neusel. "Cryptanalysis of a system using matrices over group rings." *Groups Complex. Cryptol.*, 7 (2015), pp. 175–182.

**(3)** C. Monico, M. D. Neusel. "Vector invariants of $\mathrm{Syl}_p(\mathrm{GL}(n, \mathbb{F}_q))$ and their Hilbert ideals." *Adv. Math.*, 285 (2015), pp. 1619–1629.

**(4)** P. Hadjicostas, C. Monico. "A new inequality related to the Diaconis-Graham inequalities and a new characterisation of the dihedral group." *Australas. J. Combin.*, 63 (2015), pp. 226–245.

**(5)** A. Biswas, C. Monico. "Limiting value of higher Mahler measure." *J. Number Theory*, 143 (2014), pp. 357–362.

**(6)** P. Hadjicostas, C. Monico. "A re-examination of the Diaconis-Graham inequality." *JCMCC*, 87 (2013), pp. 275–295.

**(7)** C. Monico, M. Elia. An additive characterization of fibers of characters on $\mathbb{F}_p^*$. *International Journal of Algebra*, 4:3 (2010), pp. 109–117.

**(8)** A. Farooqi, R. Gale, S. Reddy, B. Nutter, C. Monico. Markov source based test length optimized SCAN-BIST architecture. *10th International Symposium on Quality Electronic Design (ISQED 2009)*, pp. 708–713. IEEE 2009.

**(9)** M. Peterson, C. Monico. $\mathbb{F}_2$ Lanczos revisited. *Linear Algebra and Its Applications,* 428:4 (2008), 1135–1150.

**(10)** M. Elia, C. Monico. On the representation of primes in $\mathbb{Q}(\sqrt{2})$ as sums of squares. *JP Journal of Algebra, Number Theory and Applications,* 8:1 (2007), 121–133.

**(11)** G. Maze, C. Monico, J. Rosenthal. Public key cryptography based on semigroup actions. *Advances in Mathematics of Communications*, 1:4 (2007), 491–509.

**(12)** C. Monico, M. Elia. Note on an additive characterization of quadratic residues modulo $p$. *Journal of Combinatorics, Information, and System Sciences,* v.31 (2006), 209–215.

**(13)** C. Monico. On finite congruence-simple semirings. *J. of Algebra* 271 (2004), 846–854, doi:10.1006/jabr.2000.8483.

**(14)** E. Byrne, C. Kelley, C. Monico, J. Rosenthal. Non-linear codes for belief propagation. In *Proceedings of the 2003 IEEE International Symposium on Information Theory*, page 43, Yokohama, JAPAN, 2003.

**(15)** C. Monico. Computing the primary decomposition of zero-dimensional ideals. *J. of Symbolic Computation*, 34:5 (2002) 451–459.

**(16)** G. Maze, C. Monico, J. Climent, J. Rosenthal. Public-key cryptography based on simple modules over simple rings. *Proceedings of MTNS 2002.*

**(17)** G. Maze, C. Monico, J. Rosenthal. A public-key cryptosystem based on actions by semigroups. In *Proceedings of the 2002 IEEE International Symposium on Information Theory*, page 266, Lausanne, Switzerland, 2002.

**(18)** C. Monico, J. Rosenthal, A. Shokrollahi. Using low density parity check codes in the McEliece cryptosystem. *Proceedings 2000 IEEE International Symposium on Information Theory.*

**Selected Talks Given**

"Primality testing/proving" and "GNFS factorization", series of talks given at 2004 IMA Workshop on Coding Theory and Cryptography, University of Notre Dame, 6/2004.

"ECCp-109: An excursion in Internet-distributed computing". Colloquium, Texas Tech University, 1/29/04.

"Public-key cryptography via algebra and number theory." Texas Tech University, 19th Annual Fall SIAM Symposium, November 20, 2003.

"Factoring Polynomials by Numerical Methods." AMS Meeting # 985, Indiana University, Bloomington, April 4, 2003.

"Public-Key Cryptography : Where are we and where do we go from here?". Colloquium, Texas Tech University, 11/2002.

"Nonlinear Belief Propagation Decodable Codes" & "The Caveats of Generalizing Public-Key Cryptosystems". The Ohio State University, 10/2002.

"Computing the Primary Decomposition of Zero-Dimensional Ideals." 966th Meeting of the American Mathematical Society, Stevens Institute of Technology, 4/2001.

"Using Low Density Parity Check Codes in the McEliece Cryptosystem." 2000 IEEE International Symposium on Information Theory, Sorrento, Italy. 6/2000.

**Teaching Experience**

I have taught undergraduate courses including Discrete Mathematics, Contemporary Mathematics, Calculus I,II, and III, Linear Algebra, ODE I and II for engineers, Fundamentals of Computing (one `C` programming course and one course in MAPLE), Introduction to Proof, Elementary Problem Solving (for teachers), Elementary Number Theory, Abstract Algebra I and II, Intro. Real Analysis I and II, and an introductory cryptology course.

At the graduate level I have taught courses including Real Analysis I and II, Intermediate Analysis I and II, Analytic Number Theory, Elementary Number Theory, Cryptology, Fundamentals of Computing, Modern Algebra (for teachers), and Solvability by Radicals (for teachers). In Summer 2011, I also co-taught an integrated physics and math course for teachers with David Lamp, as well as a course on algebraic structures for teachers. Student evaluations of my courses are consistently above average at the departmental and college levels (numerical summaries available upon request).

**Students directed**

- Katie Bishop, "Iteration functions for Pollard's rho method on elliptic curve groups", M.S. Thesis, 5/2016.
- Ashley Ray, "A representation of Chaocipher", M.S. Thesis, 6/2012.
- Kristine Seaman, "Kryptos", M.S. Thesis, 3/2012 (co-directed with M. Neusel).
- Ernee Kozyreff, "Gröbner bases and the ideal membership problem", M.S. report 3/2012.
- Robert Danhof, "A primer on the elliptic curve method", M.S. report 4/2011.
- Bo Gilbert, "Properties of happy numbers", M.S. report 2/2011 (co-directed with R. Barnard).
- Arunabha Biswas, "A report on the state of Grimm's conjecture", M.S. report 11/2010 (co-directed with R. Barnard).
- Ronnie Williams, "Cubic polynomials for the number field sieve", M.S. Thesis, 5/2010.
- Tong Zhan, "On rainbow solutions to an equation with a quadratic term", *Integers* 9:6 (2009) 655–670. (High school student mentored at TTU as part of the Clark Scholars Program).
- Raymond Dick, "An additive characterization of quadratic residues in finite fields", M.S. Thesis, 5/2009.
- Aftab Farooqi, "Markov source based test length optimized SCAN-BIST Architecture", Ph.D. Thesis, 8/2008 (co-directed with R. Gale).
- Steven Lawless, "Super-Resolution by Local Function Approximation", M.S. Thesis, 12/2007.
- Anton Badev, "Constructing utility functions in infinite-dimensional Banach spaces", M.S. report, 8/2007.
- Memet Bulut, "Cryptography: an introduction to Schoof's algorithm", M.S. report, 5/2007.
- Michael Peterson, "Parallel block Lanczos for solving large binary systems", M.S. Thesis, 8/2006.

- Brian Miller, "A construction and analysis of arithmetic progression-free sequences", M.S. Thesis, December 2004.
- Michael Peterson, "The general number field sieve", Senior Honors Thesis, December 2004.

**Grants, Honors and Memberships**

- Awarded (TTU) "President's Excellence in Teaching Award", April 2014.
- Awarded "Graduate Professor of the Year, 2012-2013" by the TTU chapter of SIAM (departmental, awarded by graduate students).
- Awarded "Hemphill Wells New Professor Excellence in Teaching Award", 2007 (university-wide award, one per year, awarded by the TTU Parents Association).
- Awarded "Professor of the Year, 2007" by TTU Chapter of Kappa Mu Epsilon (departmental, awarded by former undergraduate students).
- Awarded "Graduate Professor of the Year, 2005-2006" by the TTU Chapter of SIAM (departmental, awarded by graduate students).
- Awarded "Professor of the Year, 2005" by the TTU chapter of the MAA (departmental, awarded by undergraduate students).
- Awarded TTU (internal) REF grant $2500 for proposal: "The distribution of quadratic non-residues", 4/2005.
- Awarded TTU (internal) REF grant $2974 for proposal: "Factoring integers with the number field sieve", 4/2004.
- Solved Certicom's $10,000 "ECC2-109" elliptic curve cryptography challenge, 4/2004.
- Solved Certicom's $10,000 "ECCp-109" elliptic curve cryptography challenge, representing the (then) new world record in elliptic curve discrete logarithm computation, 11/2002. Press coverage by CNN.com, Reuters, Slashdot, The South Bend Tribune, NBC local news, and others.
- Awarded fellowship for 2001-2002 from the Center for Applied Mathematics at the University of Notre Dame.
- SGI Award for Visualization and Computational Sciences, 2001 (only recipient from the College of Science at Notre Dame).

**Committees and Service**

- Cryptology area editor for *Journal of Algebra Combinatorics Discrete Structures and Applications.*

- Refereed several papers per year since 2004 for multiple journals and conferences, including *IEEE Trans. IT*, *Linear Algebra and Its Applications*, *Communications in Algebra*, *European Journal of Combinatorics*, *Journal of Algebra and Its Applications*, *Journal of the Australian Mathematical Society*, *Advances in Mathematics of Communications*, *Rocky Mountain Journal of Mathematics*, *J. Difference Equations and Applications*, *Finite Fields and Their Applications*.
- External examiner for Ph.D. dissertation of Urs Wagner, Universität Zürich, 7/2013.
- (College of) Arts and Sciences Committee on Academic Programs (appointed), Fall 2009-2013.
- Departmental Hiring Committee, 2012–2013 (appointed).
- Departmental Strategic Planning Committee, Spring 2012 (appointed).
- Co-organized "Topological Graph Theory" seminar with Carl Seaquist, Fall 2009–Spring 2010.
- Served on the Department of Mathematics and Statistics Graduate Committee (elected), Fall 2007– Spring 2009, and Fall 2011–2013.
- Serving on the Department of Mathematics and Statistics Noether Day Committee (appointed), Spring 2006– present.
- Served on the Department of Mathematics and Statistics Undergraduate Committee (elected), Fall 2005– Spring 2007, and Fall 2008–Spring 2010, Fall 2011–2013.
- Department of Mathematics and Statistics Executive Committee (elected), Fall 2009 – Spring 2011.
- Department of Mathematics and Statistics ad-hoc hiring steering committee (appointed), Spring 2011.
- Faculty advisor to Texas Tech chapter of the MAA (by student nomination), 2005–2008.
- Served on the Department of Mathematics and Statistics Information Technology Committee (appointed), 2003–2005, 2008–present.
- Head judge in the Computer Science category for the Exxon Mobil Texas Science and Engineering Fair, 4/2/2004.
- Organized "Cryptography and Number Theory" seminar, Fall 2003 at Texas Tech University.
- Served as mentor for students at high school (Clark Scholar program, TTU Summer Math Academy), undergraduate (SPMS program), and graduate level.