Chris Monico

December 6, 2023

Curriculum vitae

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 1996–1997	Teaching Assistantship, University of Notre Dame.
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

Most of my focus in recent years has been on cryptanalysis of public-key cryptosystems. Distilled down to simplest terms: cryptographers choose (or invent) a computational mathematical problem which they believe should require an exponential amount of time to solve, but for which it is possible to ‘reverse-engineer’ some particular solutions. They use this to build a public-key cryptosystem which can be used to secure communications. Cryptanalysts attempt to find efficient ways to solve this difficult problem, or show that the proposed cryptosystem can be defeated in some other way. The role of cryptanalysts is not antagonistic at all - they play a completely necessary role.

Should some entity manage to build a sufficiently general and powerful quantum computer, the major cryptographic systems in use today would immediately be rendered insecure; so there has been a steady stream of proposals for new schemes to replace the current ones. Unfortunately, we cannot prove any reasonable lower bounds on the complexity of the interesting mathematical problems on which most cryptosystems are built. When a new system is proposed, we initially have little more than intuition and experience advising us to whether or not it is secure. We have to assume that well-resourced adversaries will attempt to quietly 'break' the scheme so that they may use intercepted information for their own interests. Our current resolution for this issue is a 'survival of the fittest' approach. New systems are proposed by cryptographers and attacked by cryptanalysts. Those which have been attacked by many cryptanalysts over a period of years and still survive are potential candidates for actual real-world use. At present, I've contributed fatal attacks for 18 such proposed cryptographic schemes (8 published, 10 through refereeing and/or personal communication), most of which have been very algebraic in nature.

Publications

Student coauthors are indicated in bold.

(1) D. R. L. Brown, C. Monico. "More forging (and patching) of tropical signatures." *preprint* https://eprint.iacr.org/2023/1837 , 2023.

(2) **M. Tharp, B. Howe, Z. Turkowski, M. McKay, A. Brito, E. Velasquez,** C. Monico, M. Klein. "Lateral Visuomotor Distortions and Their Effects on Performance Carry-Over Effects in a Simulated Laparoscopic Environment." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2023.

(3) C. Monico. "Division in the plactic monoid." *Journal of Algebra and Its Applications*, to appear. preprint here

(4) C. Monico. "Remarks on MOBS and cryptosystems using semidirect products." *preprint* (2021), https://arxiv.org/abs/2109.11426 .

(5) **D. Rudy**, C. Monico. "Remarks on a tropical key exchange system." *J. Math. Cryptol.*, 15 (2021), pp. 280–283.

(6) C. Monico, A. Mahalanobis. "A remark on MAKE – a Matrix Action Key Exchange." *preprint* (2020), https://arxiv.org/abs/2012.00283 .

(7) C. Monico. "Cryptanalysis of a hash function, and the modular subset sum problem." *Groups, Complex. Cryptol.*, 11 (2019), 17–23. preprint here.

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

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

(10) 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.

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

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

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

(14) 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.

(15) **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.

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

(17) 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.

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

(19) 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. preprint here.

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

(21) 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.

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

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

(24) 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.

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

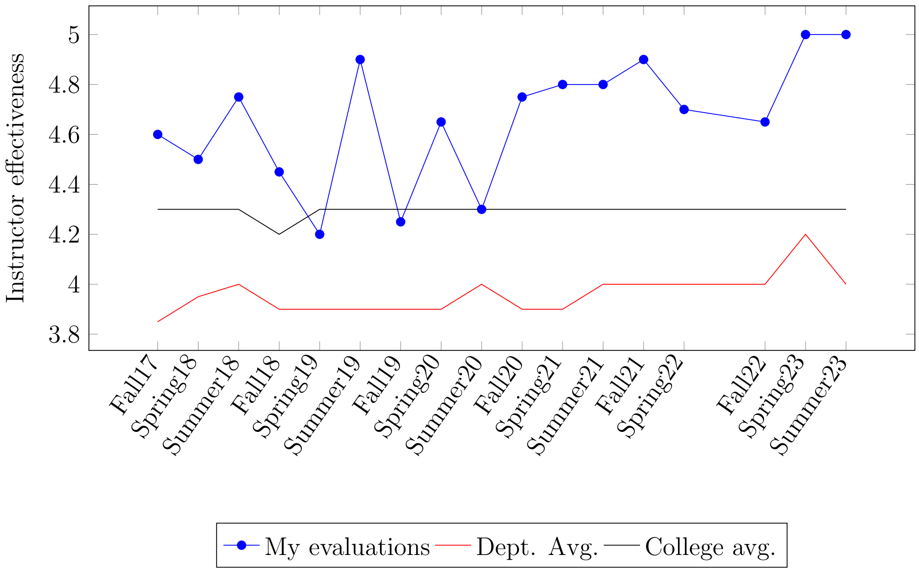
Teaching Experience

I have taught undergraduate courses including College Algebra, Discrete Mathematics, Contemporary Mathematics, Calculus I/II/III, Linear Algebra, ODE I/II for engineers, Mathematical Computing (in `C`, and in Python), Introduction to Proof, Elementary Problem Solving (for teachers), Elementary Number Theory, Abstract Algebra I/II, Intro. Real Analysis I/II, Complex Analysis, Introductory Cryptology, and a course in deep learning with TensorFlow.

At the graduate level I have taught courses including Intermediate Analysis I/II, Real Analysis I/II, Analytic Number Theory, Elementary Number Theory, Cryptology, Fundamentals of Computing, and a course in deep learning with TensorFlow. As part of our MA/Certificate programs, I have developed and taught distance graduate courses, with an audience consisting primarily of secondary teachers, in Modern Algebra and Solvability by Radicals, History of Mathematics, Modern Geometry, and Mathematical Programming. In Summer 2011, I also co-taught an integrated physics and math course for teachers with Prof. David Lamp, as well as a course on algebraic structures for teachers.

Student evaluations of my courses are generally above average at the departmental and college levels; below is a plot summarizing recent student evaluations of my courses ('Instructor effectiveness'), together with the departmental and College of Arts and Sciences averages, for reference.[1]

[1] I did also teach in Summer 2022, but the enrollment was below the university minimum threshold for reporting results.



Students directed (as chair/co-chair)

- Dylan Rudy, "Vulnerabilities of some semidirect products in Diffie-Hellman key exchanges", Ph.D., 5/2021 (co-chair with Prof. Dermot McCarthy).
- Sergio Baez, "The LLL Algorithm", M.S. report, Aug. 2020.
- Yang Zhang, "An Investigation of Some Public Key Exchange Cryptosystems", Ph.D., 5/2017.
- Katie Bishop, "Iteration functions for Pollard's rho method on elliptic curve groups", M.S. Thesis, 5/2016.
- Kristilyn Peterson, "Foundations of Calculus for the young advanced students", M.A. Thesis, 5/2015 (co-chair with Prof. Carl Seaquist).
- Ashley Ray, "A representation of Chaocipher", M.S. Thesis, 6/2012.
- Kristine Seaman, "Kryptos", M.S. Thesis, 3/2012 (co-chair 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-chair with R. Barnard).
- Arunabha Biswas, "A report on the state of Grimm's conjecture", M.S. report 11/2010 (co-chair 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. https://doi.org/10.1515/INTEG.2009.052 . (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, EE Department, 8/2008 (co-chair 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 (co-chair with Prof. Alex Wang).

Additionally, I have chaired/co-chaired 17 M.A. students' portfolios, directed undergraduate research for 5 students, and served as a committee member on numerous other M.A.,M.S., and Ph.D. students' committees, including students from Industrial Engineering and Music.

Grants, Honors and Memberships

- Awarded "Professor of the Year, 2018" by the TTU chapter of the MAA (departmental, awarded by undergraduate students).

- 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

- Faculty advisor for undergraduate club *TTU Student Developers Club*, Aug. 2021 – present; served as judge for HackWesTX 2022, HackWesTX 2023 (Spring), and HackWesTX 2023 (Fall) hackathon events.
- Faculty advisor for undergraduate club *CodePath*, Sept. 2023 – present.
- Faculty advisor for undergraduate club *RaiderHacks*, Sept. 2020 – present.
- 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 •*Advances in Mathematics of Communications*, •*Applicable Algebra in Engineering, Communication, and Computing*, •*Communications in Algebra*, •*Designs, Codes and Cryptography*, •*European Journal of Combinatorics*, •*Finite Fields and Their Applications*, •*IEEE Trans. IT*, •*Information and Computation*, •*J. of Algebra and Its Applications*, •*J. of the Australian Mathematical Society*, •*J. Difference Equations and Applications*, •*J. of Mathematical Cryptology*, •*Linear Algebra and Its Applications*, •*Mathematics of Computation*, •*Rocky Mountain Journal of Mathematics*, •*Texas College Mathematics Journal*,

- Served as external examiner for three Ph.D. dissertations since 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, Fall 2023–present.

- Served on the Department of Mathematics and Statistics Noether Day Committee (appointed), Spring 2006–Spring 2023.

- 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, 2008–2015.

- 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.

Technical skills

I have been writing computer code since the days of the TI-99/4A, Atari 800XL, Apple IIe, and Commodore 64. These days, I mostly code in C and Python, but at various times in the past, I have written good amounts of code in: C++, Objective-C, Perl, Pascal, Ada, x86 assembly, and 6502 assembly.