Curriculum Vitae

Andrew M. Klapper
e-mail: klapper@cs.uky.edu

Research Areas

Cryptography, Communications, and Coding Theory: Sequences Generated by Nonlinear Feedback Shift Registers; Stream Ciphers; Covering Radii; Applications of Complexity Theory, Algebra, Algebraic Geometry, and Combinatorics.

Academic Positions

2008-2009, Director of Graduate Studies, Department of Computer Science, University of Kentucky, Lexington, KY

2001–present, Professor, Department of Computer Science, University of Kentucky, Lexington, KY.

1997–2001, Associate Professor, Department of Computer Science, University of Kentucky, Lexington, KY.

1993–1997, Assistant Professor, Department of Computer Science, University of Kentucky, Lexington, KY.

1991–1993, Assistant/Associate Professor, Computer Science Department, University of Manitoba, Winnipeg, Manitoba.

1984–1991, Assistant Professor, College of Computer Science, Northeastern University, Boston, MA.

1981–1984, Postdoctoral Fellow, Assistant Professor, Department of Mathematics and Computer Science, Clark University, Worcester, MA.

Short Term Visiting Positions

February 2007–April 2007, Short Term Visitor, Institute for Advanced Study.

January 2007–May 2007, Visiting Researcher, Princeton University.

November 2006, Scientific Researcher, Fields Institute, Toronto, Canada.

July 2001–August 2001, Senior Scientist, Institute for Mathematical Sciences, National University of Singapore.

Spring 2000, Visiting Associate Professor, Computer Science Department, Boston University.

Fall 1999, Member, Institute for Advanced Study, School of Mathematics, Princeton, NJ.

1990, Visiting Scholar, Department of Mathematics and Computer Science, Dartmouth College, Hanover, NH.

Education

PhD in Mathematics, 1982, Brown University.

Concentration: Algebraic Geometry Over p-adic Rings.

Thesis title: Canonical Subgroups of Formal Groups of Arbitrary Dimension.

Advisor: Jonathan D. Lubin, Brown University, Providence, RI.

MS in Mathematics, 1976, Stanford University, Stanford, CA.

MS in Applied Mathematics, 1975, School of Advanced Technology, SUNY at Binghamton, Binghamton, NY.

BA in Mathematics, 1974, New York University, New York, NY.

Awards and Honors

University Research Professor, University of Kentucky, 2002-2003.

Senior Member, IEEE (Information Theory Society).

Grants

"CIF:Small: Primitives for Cryptography and Communications," National Science Foundation, July 1, 2009 – June 30, 2012, $308,309

"Theory and Application of Algebraic Feedback Shift Registers," National Science Foundation, Theoretical Foundations Cluster, July 1, 2005 – June 30, 2008, $202,000.

"Fast Hardware Encryption," National Science Foundation, Networking and Communications Research Program, March 1, 2000 – February 28, 2002, $270,000.

"The Multicovering Radii of Codes," National Science Foundation, Networking and Communications Research Program, October 1, 1997 – September 30, 2000, $301,672.

"Building Tools for Secure High Volume Communications," National Science Foundation, Networking and Communications Research Program, March 1, 1995 – February 28, 1998, $153,832.

"Building Tools for Secure High Volume Communications," University of Kentucky Summer Faculty Research Fellowship, Summer 1994, $4,000.

"Public Key Cryptosystems and Properties of Pseudorandom Sequences," National Sciences and Engineering Council of Canada Grant, April 1, 1992 – June 30, 1993, $42,000.

"Pseudorandom Sequences and Cryptography," University of Manitoba Research Grants Fund #431-1725-23, December 12, 1991 – March 31, 1992, $2590.

"A Study of Pseudorandom Sequences," National Security Agency Mathematical Sciences Program Grant #MDA904-91-H-0012, June 1, 1991 – May 31, 1994, $196,700. Joint with A.H. Chan.

Books and Book Chapters

1. "Algebraic Shift Register Sequences," by M. Goresky and A. Klapper, book draft, http://www.cs.uky.edu/∼klapper/algebraic.html (∼500 pages).

2. "Pseudorandom Number Generation," Chapter 42 in *CRC Handbook of Algorithms and Theory of Computation*, Mikhail Atallah, ed.

Refereed Journal Articles

1. "Arithmetic Correlations and Walsh Transforms," by A. Klapper and M. Goresky, submitted to *IEEE Trans. Info. Theory.*

2. "Statistical properties of the Arithmetic Correlation of Sequences," by M. Goresky and A. Klapper, in preparation.

3. "Expected π-Adic Complexity of Sequences," by A. Klapper, *IEEE Trans. Info. Theory* **56** (2010) 2486 - 2501.

4. "Lower Bounds On Error Complexity Measures For Periodic LFSR and FCSR Sequences," by R. Kavuluru and A. Klapper, *Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences* **1** (2009) 95-116.

5. "The Two Covering Radius of the Two Error Correcting BCH Code," by A. Klapper and A. Mertz, *Advances in Mathematics of Communications* **3** (2009) 83-95.

6. "The Asymptotic Behavior of 2-Adic Complexity," by A. Klapper, *Advances in Mathematics of Communications* **1** (2007) 307-319.

7. "Linear Complexity of Sequences under Different Interpretations," by A. Klapper, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **E89-A** (2006) 2254-2257.

8. "Pseudonoise sequences based on algebraic feedback shift registers," by M. Goresky and A. Klapper, *IEEE Trans. Info. Theory* **52** (2006) 1649-1662.

9. "A Survey of Feedback with Carry Shift Registers," by A. Klapper, *Sequences and Their Applications - SETA 2004*, *Springer-Verlag Lecture Notes in Computer Science* **3486** (2005) 56-71.

10. "Randomness and Register Synthesis for AFSRs based on Function Fields," by A. Klapper, *Sequences and Their Applications - SETA 2004*, *Springer-Verlag Lecture Notes in Computer Science* **3486** (2005) 282-297.

11. "On Decimations of ℓ-Sequences," by M. Goresky, A. Klapper. R. Murty, and I. Shparlinski, *SIAM Journal on Discrete Math* **18** (2004) 130-140.

12. "Periodicity and Correlations of of d-FCSR Sequences," by M. Goresky and A. Klapper, *Designs, Codes, and Cryptography* **33** (2004) 123-148.

13. "Improved Multicovering Bounds from Linear Inequalities and Supercodes," by A. Klapper, *IEEE Transactions on Information Theory* **50** (2004) 532-536. (Full version of Conference Papers 16 and 20.)

14. "Distribution Properties of d-FCSR Sequences," by A. Klapper, *Journal of Complexity* **20** (2004) 305-317.

15. "Spectral Methods for Cross-Correlations of Geometric Sequences," by A. Klapper and C. Carlet, *IEEE Transactions on Information Theory* **50** (2004) 229-232. (Full version of Conference Paper 18.)

16. "Efficient Multiply-with-Carry Random Number Generators with Optimal Distribution Properties," by M. Goresky and A. Klapper, *ACM Transactions on Modeling and Computer Simulation* **16** (2003) 310-321.

17. "Fibonacci and Galois Representations of Feedback with Carry Shift Registers," by M. Goresky and A. Klapper, *IEEE Transactions on Information Theory* **48** (2002) 2826-2836. (Full version of Conference Paper 17.)

18. "Register Synthesis for Algebraic Feedback Shift Registers Based on Non-Primes," by A. Klapper and J. Xu, *Designs, Codes, and Cryptography* **31** (2004) 227-250. (Full version of Conference Paper 22.)

19. "Multicovering Bounds from Relative Covering Radii," by I. Honkala and A. Klapper, *SIAM Journal on Discrete Math* **15** (2002) 228-234. (Full version of Conference Paper 21.)

20. "On Correlations of a Family of Generalized Geometric Sequences," with by W. Sun, A. Klapper, and Y. Yang, *IEEE Transactions on Information Theory* **47** (2001) 2609-2618.

21. "Bounds for the Multicovering Radii of Reed-Muller Codes with Applications to Stream Ciphers," by I. Honkala and A. Klapper, *Designs, Codes, and Cryptography* **23** (2001) 131-145. (Full version of Conference Paper 23.)

22. "On the Existence of Secure Keystream Generators," by A. Klapper, *Journal of Cryptology* **14** (2001) 1-15.

23. "Fourier Transforms and the 2-adic Span of Periodic Binary Sequences," by M. Goresky, A. Klapper, and L. Washington, *IEEE Transactions on Information Theory* **46** (2000) 687-691 (Full version of Conference Paper 25.)

24. "Algebraic Feedback Shift Registers," by A. Klapper and J. Xu, *Theoretical Computer Science* **226** (1999) 61-93.

25. "Improved Lower Bounds for Multicovering Codes," by A. Klapper, *IEEE Transactions on Information Theory* **45** (1999) 2532-2534.

26. "The Multicovering Radii of Codes," by A. Klapper, *IEEE Transactions on Information Theory* **43** (1997) 1372-1377. (Full version of Conference Paper 26.)

27. "Arithmetic Cross-Correlations of FCSR Sequences," by M. Goresky and A. Klapper, *IEEE Transactions on Information Theory* **43** (1997) 1342-1346.

28. "Feedback Shift Registers, 2-Adic Span, and Combiners With Memory," by A. Klapper and M. Goresky, *Journal of Cryptology* **10** (1997) 111-147.

29. "Cross-Correlations of Quadratic Form Sequences in Odd Characteristic," by A. Klapper, *Designs, Codes, and Cryptography* **11** (1997) 1-17.

30. "Large Families of Sequences with Low Correlations and Large Linear Span," by A. Klapper, *IEEE Transactions on Information Theory* **42** (1996) 1241-1248. (Full version of Conference Paper 30.)

31. "Partial Period Cross Correlations of Geometric Sequences," by A. Klapper, *IEEE Transactions on Information Theory* **IT-42** (1996) 256-260. (Full version of Conference Paper 33.)

32. "*d*-Form Sequences: Families of Sequences with Optimal Correlation Values and Large Linear Span," by A. Klapper, *IEEE Transactions on Information Theory* **41** (1995) 423-431. (Full version of Conference Paper 32.)

33. "Algebraic Nonlinearity and Its Application to Cryptography," with by L. O'Connor and A. Klapper, *Journal of Cryptology* **7** (1994) 213-228.

34. "Partial Period Autocorrelations of Geometric Sequences," by A. Klapper and M. Goresky, *IEEE Transactions on Information Theory* **IT-40** (1994) 494-502.

35. "The Vulnerability of Geometric Sequences Based on Fields of Odd Characteristic," by A. Klapper, *Journal of Cryptology* **7** (1994) 33-51. (Full version of Conference Paper 34.)

36. "Cross-Correlations of Geometric Sequences in Characteristic Two," by A. Klapper, *Designs, Codes, and Cryptography* **3** (1993) 347-377. (Extended abstract appears in Item 36.)

37. "Cascaded GMW Sequences," by A. Klapper, A. Chan, and M. Goresky, *IEEE Transactions on Information Theory* **IT-39** (1993) 177-183. (Full version of Conference Paper 37.)

38. "Cross-Correlations of Linearly and Quadratically Related Geometric Sequences and GMW Sequences," by A. Klapper, A. Chan, and M. Goresky, *Discrete Applied Mathematics* **46** (1993) 1-20.

39. "Distributed Event Algebras," by A. Klapper, *Journal of Computer and System Sciences* **44** (1992) 411-424.

40. "A New Index for Polytopes," by M. Bayer and A. Klapper, *Discrete and Computational Geometry* **6** (1991) 33-47.

41. "On the Linear Complexity of Feedback Registers," by A. Chan, M. Goresky, and A. Klapper, *IEEE Transactions on Information Theory* **36** (1990) 640-645. (Full version of Conference Paper 40.)

42. "Generalized Lowness and Highness and Probabilistic Complexity Classes," by A. Klapper, *Mathematical Systems Theory* **22**(1) (1989) 37-46.

43. "Selmer Group Estimates Arising from the Existence of Canonical Subgroups," by A. Klapper, *Compositio Mathematica* **71** (1989) 121-137.

44. "A Lower Bound on the Complexity of the Convex Hull Problem for Simple Polyhedra," by A. Klapper, *Information Processing Letters* **25** (1987) 159-161.

Refereed Conferences

1. "Non-Binary Feedback with Carry Registers and Algebraic Feedback Registers," by M. Goresky and A. Klapper, Workshop on Codes and Cryptography, Paris, France, April 2011.

2. "A With-Carry Walsh Transform (Extended Abstract)," by A. Klapper and M. Goresky, in C. Carlet and A. Pott, eds., *Sequences and Their Applications – SETA 2010, Lecture Notes in Computer Science* **6338** (2010) 217-228.

3. "Counting Functions for the k-error Linear Complexity of 2^n-Periodic Binary Sequences," by R. Kavuluru and A. Klapper, Selected Areas in Cryptography 2008.

4. "Some Results on the Arithmetic Correlation of Sequences (Extended Abstract)," by M. Goresky and A. Klapper, in S. Golomb, M. Parker, A. Pott, and A. Winterhof, eds., *Sequences and Their Applications - SETA 2008, Lecture Notes in Computer Science* **5203** (2008) 71-80.

5. "Expected π-Adic Complexity of Sequences," by A. Klapper, in S. Golomb, M. Parker, A. Pott, and A. Winterhof, eds., *Sequences and Their Applications - SETA 2008, Lecture Notes in Computer Science* **5203** (2008) 219-229.

6. "On the k-operation Linear Complexity of Periodic Sequences", by R. Kavuluru and A. Klapper, *Progress in Cryptology INDOCRYPT 2007, Lecture Notes in Computer Science* **4859** (2007) 322-330.

7. "The Asymptotic Behavior of π-Adic Complexity with $\pi^2 = -2$," by A. Klapper, in S. Golomb, G. Gong, T. Helleseth, and H.-Y. Song, ed., *Sequences, Subsequences, and Consequences, Lecture Notes in Computer Science* **4893** (2007) 134-147.

8. "Periodicity and Distribution Properties of Combined FCSR Sequences," by M. Goresky and A. Klapper, *Sequences and Their Applications SETA 2006, Lecture Notes in Computer Science* **4086** Springer-Verlag, 2006, pp. 334-341.

9. "The Two Covering Radius of the Two Error Correcting BCH Code," by A. Klapper and A. Mertz, IEEE International Symposium on Information Theory, Seattle, WA, July 2006.

10. "Linear Complexity of Sequences under Different Interpretations," by A. Klapper, International Workshop on Sequence Design and Applications, Shimonoseki Japan, 2005.

11. "The Asymptotic Behavior of 2-Adic Complexity," by A. Klapper, Workshop on Codes and Cryptography, Bergen 2005.

12. "Randomness and Register Synthesis for AFSRs based on function fields," by A. Klapper, International Conference on Sequences and Their Applications (SETA), Seoul Korea, 2004.

13. "Pseudonoise Sequences Based on Algebraic Function Fields," by A. Klapper, International Symposium on Information Theory (ISIT), Seoul Korea, 2004.

14. "A New Class of Pseudonoise Sequences," by M. Goresky and A. Klapper, International Symposium on Information Theory (ISIT), Chicago, USA, 2003.

15. "Upper Bounds on the Numbers of Resilient Functions and of Bent Functions," by C. Carlet and A. Klapper, 23rd Symposium on Information Theory in the BENELUX.

16. "Multicovering Bounds from Supercodes," by A. Klapper, International Symposium on Information Theory (ISIT) 2001. (Presentation of parts of Journal Article 13.)

17. "Galois Mode Implementation of Feedback with Carry Shift Registers," by M. Goresky and A. Klapper, International Symposium on Information Theory (ISIT) 2001. (Presentation of Journal Article 17.)

18. "Spectral Methods for Cross-Correlations of Geometric Sequences," by A. Klapper, International Conference on Sequences and Their Applications (SETA) 2001. (Presentation of Journal Article 15.)

19. "On the Distinctness of Decimations of ℓ-Sequences," by M. Goresky, A. Klapper, and R. Murty, *Proceedings of International Conference on Sequences and Their Applications (SETA) 2001*, Springer-Verlag.

20. "Multicovering Bounds from Linear Inequalities," by A. Klapper, Workshop on Codes and Cryptography (WCC) 2001, Paris, January, 2001. (Extended abstract of parts of Journal Article 13.)

21. "Multicovering Bounds from Relative Covering Radii," by I. Honkala and A. Klapper, International Symposium on Information Theory (ISIT) 2000, Sorrento, Italy, June, 2000. (Presentation of Journal Article 19.)

22. "Cryptanalysis of Stream Ciphers by Register Synthesis," by A. Klapper, *Workshop on Cryptography and Computational Number Theory*, Singapore, Dec. 22-26, 1999. (Presentation of Journal Article 18.)

23. "Multicovering Radii of Reed-Muller Codes and the Existence of Secure Stream Ciphers (Extended Abstract)," by I. Honkala and A. Klapper, *Proceedings of International Conference on Sequences and their Application (SETA), Singapore, December 1998*, Springer-Verlag, 1999. (Extended abstract of Journal Article 21.)

24. "Feedback with Carry Shift Registers over $Z/(N)$," by A. Klapper and J. Xu, *Proceedings of International Conference on Sequences and their Application (SETA), Singapore, December 1998*, Springer-Verlag, 1999, pp. 379-392.

25. "Fourier Transformations and the 2-adic Span of Periodic Binary Sequences," by M. Goresky, A. Klapper, and L. Washington, International Symposium on Information Theory (ISIT), Boston, MA, August 1998. (Presentation of Journal Article 23.)

26. "The Multicovering Radii of Codes," by A. Klapper, *Proceedings of Thirty-Fourth Allerton Conference on Communication and Control,* Urbana-Champaign, Illinois, October 1996. (Extended abstract of Journal Article 26.)

27. "On the Existence of Secure Feedback Registers," by A. Klapper, *Advances in Cryptology – Eurocrypt 1996, Lecture Notes in Computer Science* **1070** Springer-Verlag, 1996, pp. 256-267.

28. "Cryptanalysis Based on 2-Adic Rational Approximation," by A. Klapper and M. Goresky, *Advances in Cryptology – CRYPTO '95, Lecture Notes in Computer Science* **963** Springer-Verlag, 1995, pp. 262-273.

29. "Large Period Nearly deBruijn FCSR Sequences," by A. Klapper and M. Goresky, *Advances in Cryptology – Eurocrypt 1995, Lecture Notes in Computer Science* **921** Springer-Verlag, 1995, pp. 263-273.

30. "Large Families of Sequences with Low Correlations and Large Linear Span," by A. Klapper, *Proceedings of the Thirty-Second Allerton Conference on Communication and Control*, Urbana-Champaign, Illinois, September 1994, pp. 464-472. (Extended abstract of Item 30.)

31. "Feedback Registers Based on Ramified Extensions of the 2-Adic Numbers," by M. Goresky and A. Klapper, *Advances in Cryptology – Eurocrypt 1994, Lecture Notes in Computer Science* **718** Springer-Verlag, 1994, pp. 215-222.

32. "d-Form Sequences: Families of Sequences with Optimal Correlation Values and Large Linear Span," by A. Klapper, *Proceedings of the Thirty-First Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, Ill, Sept., 1993, pp. 625-634. (Extended abstract of Item 32.)

33. "Partial Period Cross Correlations of Geometric Sequences," by A. Klapper, *Proceedings of the Thirty-First Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, Ill, Sept., 1993, pp. 635-642. (Extended abstract of Item 31.)

34. "The Vulnerability of Geometric Sequences Based on Fields of Odd Characteristic," by A. Klapper, *Advances in Cryptology – Auscrypt '92, Lecture Notes in Computer Science* **718** Springer-Verlag, 1993, pp. 327-338. (Extended abstract of Item 35.)

35. "Revealing Information with Partial Period Autocorrelations," with by A. Klapper and M. Goresky, *Proceedings, Asiacrypt '91*, Fujyoshida, Japan, Nov. 1991.

36. "Cross-Correlations of Geometric Sequences in Characteristic Two," by A. Klapper, *Proceedings, International Symposium on Information Theory and its Applications*, Waikiki, Hawaii, Nov. 1990. (Extended abstract of Item 36.)

37. "Cascaded GMW Sequences," by A. Klapper, A. Chan, and M. Goresky, *Proceedings of the Twenty-Eighth Annual Allerton Conference on Communication Control and Computing*, Urbana-Champaign, Ill, Oct. 1990, pp. 1008-1013. (Extended abstract of Item 37.)

38. "Cross-Correlations of Linearly and Quadratically Related Geometric Sequences and GMW Sequences," by A. Chan and M. Goresky, and A. Klapper, Marshall Hall Memorial Conference, Burlington, Vermont, Sept. 1990.

39. "Correlation Functions of Geometric Sequences," by A. Chan, and M. Goresky and A. Klapper, *Advances in Cryptology – Eurocrypt '90, Lecture Notes in Computer Science* **473** Springer-Verlag, 1991, pp. 214-221.

40. "On the Linear Complexity of Feedback Registers," by A. Chan, and M. Goresky and A. Klapper, *Advances in Cryptology – Eurocrypt '89, Lecture Notes in Computer Science* **434** Springer-Verlag, 1990, pp. 563-570. (Extended abstract of Item 41.)

Unrefereed Conferences and Invited Workshops

1. "Algebraic Feedback Shift Registers," by A. Klapper, International Workshop on Codes and Cryptography, Wuyishan, China, June, 2007.

2. "Feedback with Carry Shift Registers over Finite Fields," by A. Klapper, *Proceedings of Leuven Algorithms Workshop, Lecture Notes in Computer Science* **1008** Springer-Verlag, 1994, pp. 170-178.

3. "Feedback with Carry Shift Registers – 2-Adic Models and Summation Combiners," by A. Klapper and M. Goresky, *Proceedings, 1994 IEEE International Symposium on Information Theory,* Trondheim, Norway, June, 1994.

4. "2-Adic Shift Registers and the Security of Stream Ciphers ," by A. Klapper, *Midwest Theory Day,* Indianapolis, IN, April, 1994.

5. "2-Adic Shift Registers," by A. Klapper, M. Goresky, *Fast Software Encryption: Proceedings of 1993 Cambridge Algorithms Workshop, Lecture Notes in Computer Science* **809** Springer-Verlag, 1994, pp. 174-178.

6. "On the Autocorrelation Functions of Binary Sequences Obtained from Finite Geometries," by A. Chan, A. Klapper, and M. Goresky, IEEE International Symposium on Information Theory, San Diego, CA, Jan. 1990.

7. "Feedback Registers as Polynomials," by A. Chan, H. Fell, and A. Klapper, and M. Goresky, *EISS Workshop on Stream Ciphers,* Karlsruhe, January 1989.

Technical Reports Not Appearing Elsewhere

1. "Correlation Functions of Geometric Sequences," by A. Chan, M. Goresky, A. Klapper, Northeastern University, College of Computer Science Technical Report NU-CCS-90-3 (1990).

2. "Approximating Convex Hulls of Finite Sets of Curves," by A. Klapper, Northeastern University, College of Computer Science Technical Report NUCCS-87-11 (1987).

3. "Unimaximality and the Symmetric All-Furthest-Neighbors Problem," by A. Klapper, Northeastern University, College of Computer Science Technical Report NUCCS-87-13 (1987).

Invited Talks

1. "Feedback with Carry Shift Registers," Plenary talk, Sequences and Their Applications (SETA), 2004, Seoul, Korea.

2. "Polynomial Generalizations to Linear Feedback Shift Registers," Conference on Polynomial-Based Cryptography, Melbourne, Australia, July 2004.

3. "Linear Complexity is Just the Tip of the Iceberg: Security Measures for Stream Ciphers," University of Illinois at Urbana-Champaign, March 2004.

4. "Randomness of Sequence Defined by Algebraic Feedback Shift Registers," University of Illinois at Urbana-Champaign, March 2004.

5. "Linear Complexity is Just the Tip of the Iceberg: Security Measures for Stream Ciphers," University of Calgary, August 2003.

6. "Pseudorandom Sequences Based on Algebraic Structures," Workshop On Random Number Generators and Highly Uniform Point Sets, Montreal, Canada, June 2002.

7. "Linear Complexity is Just the Tip of the Iceberg: Security Measures for Stream Ciphers," Plenary Talk, Indocrypt 2001, Madras, India, December 2001.

8. "Periodicity, correlation, and distribution properties of d-FCSR sequences," National University of Singapore, August 2001.

9. "On the Distinctness of Decimations of ℓ-Sequences," National University of Singapore, July 2001.

10. "Algebraic Feedback Shift Registers and the Security of Stream Ciphers," Rutgers University, March 2001.

11. "Feedback with Carry Shift Registers and the Security of Stream Ciphers," Clark University, February 2001.

12. "Feedback with Carry Shift Registers and the Security of Stream Ciphers," Tufts University, April 2000.

13. "Algebraic Feedback Shift Registers and the Security of Stream Ciphers," Boston University, March 2000.

14. "Making and Breaking Codes," University Sciences Lecture, Colgate University, October, 1997.

15. "The Multicovering Radii of Codes," Dept. of Mathematics, University of Kentucky, October, 1996.

16. "Existence Results for Families of Secure Feedback Registers," Isaac Newton Institute, Cambridge University, March, 1996.

17. "2-Adic Shift Registers," University of Cincinnati, May 1994.

18. "Public Key Cryptosystems with Partial Secrecy," University of Kentucky, May, 1992.

19. "Revealing Information with Partial Period Autocorrelations," SUNY at Buffalo, October, 1991.

20. "On the Linear Complexity of Feedback Registers," Clark University, April, 1990.

21. "Correlation Functions of Geometric Sequences," Dartmouth College, March, 1990.

22. "On the Linear Complexity of Feedback Registers," Northeastern University, October, 1989.

23. "Upper Bounds on the Linear Complexity of Feedback Registers," Dartmouth College, March, 1989.

24. "Generalized Lowness and Highness and Probabilistic Complexity Classes," Clark University, April, 1988.

Teaching

Undergraduate: Introduction to Computer Science I, II; Algorithms and Data Structures I, II; Logic; Discrete Math; Systems Programming; Operating Systems I, II; Cryptography; Foundations of Computing; Analysis of Algorithms; Calculus I, II, III; Linear Algebra; Number Theory; Differential Equations.

Graduate: Algebraic Algorithms; Cryptography; Error Correcting Codes; Operating Systems I, II; Complexity Theory; Automata Theory; Theory of Computation; Assembly Language; Analysis of Algorithms.

Graduate Students: Jinzhong Xu (Ph.D., May 2000); Andrew Mertz (Ph.D., August 2005); Ramakanth Kavuluru (Ph.D. May 2009); Weihua Liu (current Ph.D. student); Ting Gu (current Ph.D. student); Jesse Andrews (Ph.D., not completed); Xiaotian Li (Ph.D., not completed); Yang Ling (Ph.D., not completed); Kim Harrison (Ph.D., not completed); Michael Ludlum (MS, 2000); Yue Lai (MS, 1999); Jonathan Edwards (MS, 1994); Peter Wilson (current MS. student); .

Community Service

Associate Editor, Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences, 2007–.

Associate Editor, Advances in Mathematics of Communications, 2006–.

Associate Editor for Sequences, IEEE Transactions on Information Theory, Dec. 1, 1999 – Dec. 31, 2002.

Associate Editor for Research, Cryptologia, Jan. 1, 1999 – July 2001.

General Chair of Sequences and Their Applications (SETA) '08.

General Chair of Crypto '98.

Member, Advisory Board, Sequences and Their Applications (SETA).

Member, Board of Directors, International Association for Cryptologic Research, 1998.

Member, IEEE Information Theory Society Subcommittee on Awards, 2005.

Program committee member, Boolean Functions: Cryptography & Applications, Copenhagen, May 2008.

Program committee member, Third International Workshop on Sequence Design and its Applications in Communications (IWSDA '07), Chengdu, China, September 2007.

Program committee member, Workshop on Sequences, Subsequences, and Consequences, University of Southern California, May 2007.

Program committee member, International Conference on Sequences and Their Applications (SETA) 2006, Beijing, China, October 2006.

Program committee member, IEEE International Symposium on Information Theory, Seattle, WA, July 2006.

Program committee member, Second International Workshop on Sequence Design and its Applications in Communications (IWSDA '05), Shimonoseki, Yamaguchi, Japan, October 2005.

Program committee member, International Conference on Sequences and Their Applications (SETA) 2004, Seoul, South Korea, October 2004.

Program committee member, International Workshop on Coding, Cryptography, and Combinatorics, Yellow Mountains, China, June 2003.

Program committee member, Indocrypt 2002, Bangalore, India.

Program committee member, International Conference on Sequences and Their Applications, Bergen, Norway, '01.

Program committee member, Indocrypt 2000, Calcutta, India.

Program committee member, Crypto '99.

Program committee member, International Conference on Sequences and Their Applications, Singapore, '98.

Program committee member, Crypto '96.

Consultant for Kentucky State Police on Cryptography.

Organizer, 1989 Northeastern University Theory Day.

Member: Assoc. for Computing Machinery; ACM SIGACT; IEEE Information Theory Society; Int. Assoc. for Cryptologic Research.

Referee for: Theoretical Computer Science; Journal of Cryptology; IEEE Transactions on Information Theory; IEEE Transactions on Communications; IEEE Transactions on Computers; Information and Control; Mathematical Systems Theory; Journal of Computer and System Sciences; Information Processing Letters; Structure in Complexity Theory Conference; National Science Foundation; Idaho State Board of Education; Northeastern University Internal Research Grants Program.

Grant review panelist, NSF.

co-Foreman and co-Founder, Squash Beetle Morris dancers, 1994-2006.

Board of Directors, Lexington Traditional Dance Association.

University Service

Member, U. Kentucky Librarians Area Committee, 2007-08.

Member, U. Kentucky Strurgill Award Committee, 2007-08.

Member, U. Kentucky Committee to Select University Research Professors, 2004-2006.

Member, U. Kentucky College of Engineering Fellowships Committee, 2004-2007.

Member, U. Kentucky College of Engineering Research Committee, 2002-2006.

Member, U. Kentucky College of Engineering Research CQI Team, 1998-99.

Member, U. Kentucky Dept. of Computer Science Director of Graduate Studies, 2008-2009.

Member, U. Kentucky Dept. of Computer Science Executive Committee, Fall 2002.

Member, U. Kentucky Dept. of Computer Science Committee on Publications, 2000-present.

Member, U. Kentucky Dept. of Computer Science, Committee on Higher Degrees, 1993-1999, 2006-present.

Member, U. Kentucky Dept. of Computer Science, Hiring Committee, 1993-1994.

U. Kentucky Dept. of Computer Science, Library Liaison, 1994-98.

Chair, U. Manitoba Dept. of Computer Science Awards Committee, 1992-1993.

Member, U. Manitoba Dept. of Computer Science Graduate Review Committee, Systems Area Teaching Committee, Foundations Area Teaching Committee.

Northeastern U., College of Computer Science Representative, Faculty Senate, 1987-89.

Chair, Northeastern U., Faculty Senate Academic Policy Committee, 1987-88.

Member of Northeastern U. Departmental Committees: Merit Raise, Curriculum, Academic Standing, Honors, Operating Systems Teaching Group, Foundations Teaching Group, Systems Teaching Group.