Biographical Information: Professor Andrew Klapper

Address: Dept. of Comp. Sci., 779A Anderson Hall, Univ. Kentucky, Lexington, KY 40506-0046.

Telephone: (859) 257-6743 (Office); (859) 323-1971 (Fax).

E-mail and web page : klapper@cs.uky.edu, `http://www.cs.uky.edu/~klapper/`

Citizenship: United States

Professional Preparation:

New York University, Mathematics, B.A. 1974.

SUNY at Binghamton, Applied Mathematics, M.S. 1975.

Stanford University, Mathematics, M.S. 1976.

Brown University, Mathematics, Ph.D. 1982. Concentration: Algebraic Geometry Over p-adic Rings. Thesis title: Canonical Subgroups of Formal Groups of Arbitrary Dimension.

Appointments:

2008 – 2009, Director of Graduate Studies, Dept. of Comp. Sci., Univ. of Kentucky

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

1993 – present, Assistant Professor/Associate Professor (1997)/Professor (2001), Department of Computer Science, University of Kentucky.

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

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

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

List of Most Important Publications:

1. "Algebraic Shift Register Sequences," M. Goresky and A. Klapper, in press, Cambridge university Press (500 page monograph).
2. "A With-Carry Walsh Transform (Extended Abstract)," 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. Polynomial Pseudo-Noise Sequences Based on Algebraic Feedback Shift Registers, M. Goresky and A. Klapper, *IEEE Trans. Info. Theory* **53** (2006) 1649-1662.
4. Distribution properties of d-FCSR sequences, A. Klapper, *Journal of Complexity* **20** (2004) 305-317.
5. Register Synthesis for Algebraic Feedback Shift Registers Based on Non-Primes, A. Klapper and J. Xu, *Designs, Codes, and Cryptography* **31** (2004) 227-250.
6. "Bounds for the Multicovering Radii of Reed-Muller Codes with Applications to Stream Ciphers," I. Honkala and A. Klapper, *Designs, Codes, and Crypto.* **23** (2001) 131-145.
7. On the Existence of Secure Keystream Generators, A. Klapper *Journal of Cryptology* **14** (2001) 1-15.

8. Algebraic Feedback Shift Registers, A. Klapper and J. Xu, *Theoretical Computer Science* **226** (1999) 61-93.
9. Arithmetic Cross-Correlations of FCSR Sequences, M. Goresky and A. Klapper, *IEEE Transactions on Information Theory* **43** (1997) 1342-1346.
10. "The Multicovering Radii of Codes," by A. Klapper, *IEEE Transactions on Information Theory* **43** (1997) 1372-1377.
11. Feedback Shift Registers, Combiners With Memory, and 2-Adic Span, A. Klapper and M. Goresky, *Journal of Cryptology* **10** (1997) 111-147.
12. "The Vulnerability of Geometric Sequences Based on Fields of Odd Characteristic," A. Klapper, *Journal of Cryptology* **7** (1994) 33-51.
13. "A New Index for Polytopes," M. Bayer and A. Klapper, *Discrete and Computational Geometry* **6** (1991) 33-47.

The above papers are available on Professor Klapper's home page.

Synergistic Activity:

General Chair, SETA 2008, Lexington, KY.

General Chair, Crypto '98, Santa Barbara, CA.

Associate Editor and member of the organizing committee, 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, 2000 – 2003.

Member of the SEquences and Their Applications (SETA) conference planning committee, 2004 – present.

Recent Collaborators:

Claude Carlet, INRIA; Mark Goresky, Institute for Advanced Study; Judy Goldsmith, University of Kentucky; Iiro Honkala, Turku University; Ramakanth Kavuluru, University of Kentucky; Nicholas Mattei, University of Kentucky; Andrew Mertz, University of Kentucky; Ram Murty, Queen's University; Igor Shparlinski, Macquarie University; Jinzhong Xu, University of Kentucky.

Recent PhD Students:

1. Ramakanth Kavuluru (PhD, 9/09; supported under NSF grant CCF-0514660)
2. Andrew Mertz (PhD, 5/06; supported under NSF grants NCR-9706078
3. Jinzhong Xu (PhD, 5/00; supported under NSF grant NCR-9400762) and CCR 9980429)
4. Weihua Liu (PhD student; supported under NSF grant)
5. Ting Gu, (PhD student; supported under NSF grant)
6. Peter Wilson (PhD student; supported under NSF grant CCF-0514660)
7. Jesse Andrews (PhD student; supported under NSF grant CCR-9980429)
8. Xiaotian Li (PhD student; supported under NSF grant CCR-9980429)

Graduate Advisor: Jonathan Lubin, Brown University