Steven Myers

Department of Computer Science
University of Toronto
10 King's College Road
Toronto, Ontario, M5S 3G4
Canada

Home:(416) 536-9679
Work:(416) 946-3923
Fax:(416) 978-1931
Email:myers@cs.toronto.edu
WWW: http://www.cs.toronto.edu/~myers

Education

Ph.D. Candidate	Computer Science, University of Toronto. Degree expected spring 2004. Advisor: Professor Charles Rackoff.
M.Sc.	Computer Science, University of Toronto, 1999. Advisor: Professor Charles Rackoff.
B.Sc. Honours	Computer Science, University of Calgary, 1997. Honours Supervisor: Professor Lisa Higham.

Professional and Research Experience

2001-Present	**Cryptographer & Developer**, E-Witness Corp., Toronto. (Part-time Employee) E-Witness is a company that develops cryptographic products for the World Wide Web
May- August 2000	**Visiting Researcher,** Cryptography and Information Security Group, Telcordia Technologies (formerly Bellcore), Morristown, New Jersey, U.S.A
January – June 1998	**Visiting Researcher**, Complexity Theory Program at the Fields Institute for Research in Mathematical Sciences, Toronto.
May- August 1997	**Research Assistant**, Department of Computer Science, University of Calgary, Calgary.
May-August 1996	**Research Assistant,** National Research Council of Canada.
May-August 1995	**Software Developer**, Fording Coal Ltd.

Research Interests

My research interests are in cryptography, systems security and computational complexity theory. I am interested in combinatorial models of private-key cryptography; theoretical and practical models of public-key cryptography; private computation and systems security. I am also interested in the fundamental relationship between complexity theory and cryptography. For a complete description please see the accompanying research statement.

Teaching Experience

- **Teaching Assistant**, University of Toronto, 1997-2003.
  Courses: 1st year introduction to computer science, 2nd year discrete-math, 3rd year introduction to algorithms, graduate cryptography, graduate theory of machine learning and graduate complexity theory.

- **Teaching Assistant,** University of Calgary, 1996-1997
  Courses: 1st year introduction to computer science, 2nd year data-structures and algorithms, 2nd year low-level programming and 2nd year hardware/software interface.

Publications

- Efficient Amplification of the Security of Weak Pseudo-Random Function Generators, Steven Myers, *Journal of Cryptology,* Vol. 16, Pages 1-24, Springer, 2003. (Extended Abstract appeared in EUROCRYPT 2001, LNCS 2045, Pages:358-372, Springer, 2001)

- Cryptographic Counters and Voting, Jon Katz, Steven Myers and Rafail Ostrovsky, *Proceedings of Advances in Cryptology—EUROCRYPT 2001*, LNCS 2045, Pages 78-92, Springer, 2001.

- On the Development of Block-Ciphers and Pseudo-Random Function Generators Using the Composition and XOR Operators, Steven Myers, *Master's Thesis and University of Toronto Technical Report*, 1999

- Self-Stabilizing Token-Circulation on Anonymous Message Passing Rings, Steven Myers, *Proceedings of the 2nd International Conference on the Principles of Distributed Systems*, Pages 115-128, Hermis, 1998.

- Models of Self-Stabilization, Steven Myers, *Honours Thesis*, 1997.

Submitted for Publication

- Simple Permutations Mix Well, Shlomo Hoory, Avner Magen, Steven Myers and Charles Rackoff, *Submitted to the 36th Symposium on Theory of Computing (STOC 04).*

- Black-Box Composition Does Not Imply Adaptive Security for Permutations, Steven Myers, *Submitted to Advanced in Cryptology-EUROCRYPT 2004.*

Presentations

- Eurocrypt, Innsbruck, Austria, 2001

- International Conference on the Principles of Distributed Systems, Amiens, France 1998

- Invited Talk, University of South Paris, France, 1998

- Workshop on Complexity Issues in Parallel and Distributed Computing, Fields Institute, Toronto, 1998

Awards

2000-2003	Ontario Graduate Scholarship
1999-2000	Ontario Graduate Scholarship in Science and Technology.
1997-1999	University of Toronto Open Fellowship.
1997	3rd Place, ACM Mountain Regional Programming Competition.
1996-1997	University of Calgary Achievement Scholarship.
1994-1997	Fording Coal Ltd. Class-A Scholarship.

References

- Professor Charles W. Rackoff
  Department of Computer Science
  University of Toronto
  Toronto, ON, M5R 3G4
  CANADA
  Phone: (416) 978-4106
  Fax: (416) 978-1931
  E-mail: rackoff@cs.toronto.edu

- Professor Rafail Ostrovsky
  UCLA Department of Computer Science
  University of California, Los Angeles
  3731 Boelter Hall,
  Los Angeles, CA, 90095-1596
  USA
  Phone: (310) 206-5283
  Fax: (310) 825-7578
  E-mail: rafail@cs.ucla.edu

- Assistant Professor Tal Malkin
  Department of Computer Science
  Columbia University
  514 CSC
  1214 Amsterdam Avenue MC 0401
  New York, NY 10027-7003,
  USA
  Phone: (212) 939-7097
  Fax: (212) 666-0140
  E-mail: tal@cs.columbia.edu

- Professor Toniann Pitassi
  Department of Computer Science
  University of Toronto
  Toronto, ON, M5R 3G4
  CANADA
  Phone: (416) 978-3695
  Fax: (416) 978-1931
  E-mail: toni@cs.toronto.edu

- Professor Ian F. Blake
  Department of Electrical and Computer Engineering
  University of Toronto
  Toronto, Ontario M5S 3G4
  CANADA
  Phone: (416) 946-5785
  Fax: (416) 978-4425
  E-mail: ifblake@comm.utoronto.ca