

SHARON GOLDBERG

<http://www.princeton.edu/~goldbe/>
goldbe@princeton.edu

ACADEMIC HISTORY

Ph.D. Candidate, Princeton University, Department of Electrical Engineering 2006-Present

Awards: Upton Fellowship (2004 – 2008)

Advisors: Jennifer Rexford (Computer Science), Boaz Barak (Computer Science)

Research areas: Network Security, Cryptography, Networking, Game theory.

- Using formal techniques from cryptography and game theory to design and model secure protocols for data networking.

M.A., Princeton University, Department of Electrical Engineering 2004-2006

Advisor: Paul R. Prucnal (Electrical Engineering)

Research area: Optical Communications

Courses: Random Processes, Queuing Theory, Coding Theory, Photonics, Cryptography.

- Developed and analyzed application of optical code division multiple access (CDMA) using techniques from queuing theory, coding theory and cryptography.

B.A.Sc., University of Toronto, Division of Engineering Science, Electrical Option 1999-2003

GPA: 3.85/4.00

Awards: Dean's Honour List (1999-2003), Jacob Felzen Scholarship (2002-2003)

INDUSTRY EXPERIENCE

Cisco Systems, Inc., Research Intern San Jose, CA, Summer 2008

- Prototyped the “secure sketch” path-quality monitoring protocol developed during my PhD research on a Cisco application services platform.
- Produced a full technical specification for the protocol.
- Worked with marketing and engineering in various business units to analyze use cases for the protocol.

IBM T.J. Watson Research, Cryptography Research Intern Hawthorne, NY, Summer 2007

- Used theoretical tools from cryptography and game theory to study security of interdomain routing protocols for the Internet.

Hydro One Networks Inc., Telecom Engineer Toronto, ON, Canada, 2003-2004

- Designed communication circuits in wireless, copper, and optical media. Selected and tested new communications devices (e.g. spread-spectrum radios). Oversaw projects from design to installation.

Bell Canada, Lead Database Designer Toronto, ON, Canada, Summer 2002

- Led a three-person team to design database application used by over 40 members of project team to track rollout of a \$300M network connecting 1,000 gov't sites. Database was used for over 4 years.

Bell Nexxia, Junior Internetworking Engineer Toronto, ON, Canada, Summer 2001

- Contributed to the design and rollout of a network of 1800 bank machines.
- Developed database application that continued to be used by the team for over 5 years.

Personification Inc., Intern Toronto, ON, Canada, Summer '99, '00

- Gathered and analyzed market data as part of product planning teams. Designed corporate website.

PUBLICATIONS

Secure Protocols for Data Networking:

- **S. Goldberg**, S. Halevi, A. Jaggard, V. Ramachandran, R. Wright, "Rationality and Traffic Attraction: Incentives for Honest Path Announcements in BGP", *ACM SIGCOMM'08*, August 2008.
- **S. Goldberg**, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path-Quality Monitoring in the Presence of Adversaries", *ACM SIGMETRICS'08*, June 2008.
- B. Barak, **S. Goldberg**, and D. Xiao, "Protocols and Lower Bounds for Failure Localization in the Internet", *LACR EUROCRYPT'08*, April 2008.
- **S. Goldberg**, J. Rexford, "Security Vulnerabilities and Solutions for Packet Sampling". *IEEE Sarnoff Symposium*, Princeton, NJ, May 2007. Our results have been incorporated into to the IETF PSAMP (Packet Sampling) Charter.

Optical Code Division Multiple Access (O-CDMA):

- **S. Goldberg**, R. Menendez, P. Prucnal, "Towards a Cryptanalysis of Spectral-Phase Encoded Optical CDMA with Phase-Scrambling". *Optical Fiber Communications Conference, OFC'07*, March 2007.
- **S. Goldberg**, P.R. Prucnal, "On the Teletraffic Capacity of Optical CDMA", *IEEE Transactions on Communications*, July 2007.
- **S. Goldberg**, V. Baby, T. Wang, P.R. Prucnal, "Source matched spreading codes for optical CDMA", *IEEE Transactions on Communications*, May 2007.

Analog Circuit Design:

- **S. Goldberg**, S. Lui, S. Nicolson, K. Phang "CMOS Limiting Optical Preamplifiers Using Dynamic Biasing for Wide Dynamic Range", *IEEE International Symposium on Circuits and Systems*, May 2004.

PRESENTATIONS

Incentives for Honest Path Announcements in BGP

Conferences: ACM SIGCOMM 2008 (Seattle, WA, 08/2008)

Workshops: DIMACS Secure Routing Workshop (New Brunswick, NJ, 02/2008)

Industry: IBM Research (Hawthorne, NY, 08/2007 and 03/2008), Cisco (San Jose, CA, 08/2008)

Academia: UC Berkeley (03/2008), Tel Aviv University (Israel 04/2008), Hebrew University (Jerusalem, Israel, 04/2008), Stanford University (08/2008), University of Toronto (08/2008)

Path-Quality Monitoring in the Presence of Adversaries

Conferences: ACM SIGMETRICS 2008 (Annapolis, MD, 06/2008)

Industry: Cisco (San Jose, CA, 03/2008 and various talks in summer 2008)

Academia: Weizmann Institute (Israel, 04/2008), Ben Gurion University (Be'er Sheva, Israel 04/2008)

Failure Detection and Localization: A Cryptographic Study of Secure Internet Measurement

Academia: Stanford University (03/2007), New York University (04/2007), University of Maryland (05/2007), Penn State University (10/2007)

Towards a Cryptanalysis of Optical CDMA with Phase Scrambling

Conferences: Optical Fiber Conference, OFC'07 (Anaheim, CA, 03/2007)

Workshops: IPAM Securing Cyberspace Program: Workshop on Hardware for Cryptography (Los Angeles, CA, 12/2006)

Industry: IBM Research (Hawthorne, NY, 01/2007) Telcordia (Red Bank, NJ, 03/2007)

PRESENTATIONS (CONTINUED)

Security Vulnerabilities and Solutions for Packet Sampling

Conferences: IEEE Sarnoff Symposium (Princeton, NJ, 05/2007)

Exploring the Benefits of CDMA in Optical Networks

Workshops: PRISM Workshop on Optical Communications Technologies (Princeton, NJ, 02/2006)

CMOS Limiting Optical Preamplifiers Using Dynamic Biasing for Wide Dynamic Range

Conferences: IEEE International Symposium on Circuits and Systems (Vancouver 04/2004)

TEACHING EXPERIENCE

ELE201 Intro to Electrical Signals & Systems, Princeton, Head Teaching Assistant Spring 2006

- Ran weekly precept. Prepared course problem sets, midterm and final exam.
- Awarded Outstanding Teaching Assistant Award (Dept. of Electrical Engineering)

ECE159 Fundamentals of Electricity & Circuits, University of Toronto, Tutor Spring 2003

- Conducted weekly tutorials with up to 100 students voluntarily in attendance.

AER201 Engineering Design, University of Toronto, Extra-Help Tutor Spring 2002

- Advised students on circuit design and troubleshooting strategies at extra-help sessions.

PROFESSIONAL SERVICE

Graduate Women in Science and Engineering, (GWISE), Princeton University

President (2007-2008), **Vice-President** (2006-2007), **Secretary** (2005-2006)

- Ran organization for female engineering graduate students with over 200 members.
- Organized bi-yearly professional development seminars, monthly networking events, and yearly welcome and graduation lunches. Mentored female graduate students.
- Participated in high school outreach events, attended conferences for women in engineering (Grace Hopper 2007), Princeton WISE Conferences (2006, 2008).

Co-organizer, Princeton/NYU High School Girls Engineering Colloquium Spring 2008

- Lead organization (with another student) of day-long colloquium on opportunities in engineering for 120 girls in 9th-10th grade at nine high schools in New York City.
- Oversaw program of over 20 speakers and demonstrations by graduate students and faculty from NYU and Princeton. Oversaw budget and secured funding from Google.

Program Committee: NetEcon'09.

External Reviewer: USENIX NSDI '09, IACR TCC '09, SODA '09, CNCC'09, IACR CRYPTO'08, ACM SIGCOMM CCR, ACM CCS'08, ANCS'08, MobiCom'08, CNCC'08, ANCS'07, ACM SIGCOMM'06.

Standards: Contributed to IETF PSAMP (Packet Sampling) Charter.

Affiliations: Engineer In Training, Professional Engineers of Ontario (PEO) 2003-Present
Student Member, Association for Computing Machinery (ACM) 2006-Present

INTERESTS

Argentine tango. Swing dance. Fiction, biographies, short stories, history. Travel.