

SHARON GOLDBERG

<http://www.cs.bu.edu/~goldbe/>
goldbe@cs.bu.edu

ACADEMIC HISTORY

Ph.D., Princeton University, Department of Electrical Engineering 2006-2009

Awards: Upton Fellowship (2004 – 2008)

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

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

Thesis: “Towards Securing Interdomain Routing on the Internet”

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.

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

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

Thesis: “A CMOS Limiting Optical Preamplifier with Wide Dynamic Range”

EMPLOYMENT

Assistant Professor, Boston University, Computer Science Department. August 2010-Present

Postdoctoral Researcher, Microsoft Research, New England. Cambridge, MA, August 2009-June 2010

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

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

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

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

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

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

PUBLICATIONS

Network Security:

- P. Gill, M. Schapira, **S. Goldberg**. “Let the Market Drive Deployment: A Strategy for Transitioning to BGP Security.” *ACM SIGCOMM*, August 2011.
- M. Lee, **S. Goldberg**, R. R. Kompella, G. Varghese “Fine-Grained Latency and Loss Measurements in the Presence of Reordering”, *ACM SIGMETRICS*, June 2011.
- **S. Goldberg**, M. Schapira, P. Hummon, and J. Rexford. “How Secure are Secure Interdomain Routing Protocols”, *ACM SIGCOMM*, August 2010.
- C. Gaspard, **S. Goldberg**, W. Itani, E. Bertino and C. Nita-Rotaru. “SINE: A Cache-Friendly Integrity Protocol for the Web”, *NPSec*, October 2009.
- **S. Goldberg**, S. Halevi, A. Jagard, 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

Let the Market Drive Deployment: A Strategy for Transitioning to BGP Security

Conferences: NANOG'52 – Meeting of the North American Network Operator's Group (06/2011)
Industry: DHS BGPsec working group (02/2011), Google Tel Aviv (05/2011)
Academia: MIT Security Seminar (02/2011), Bar Ilan University (Tel Aviv, 05/2011)
The Hebrew University of Jerusalem (05/2011), Tel Aviv University (05/2011)

Signature Options for BGPsec

Industry: DHS BGPsec working group (06/2010, 12/2010, 02/2011)
IBM Cryptography Seminar (Hawthorne, NY 04/2011)

PRESENTATIONS (CONTINUED)

How Secure are Secure Routing Protocols?

- Conferences: SIGCOMM (New Delhi, India, 08/2010)
NANOG'49 – Meeting of the North American Network Operator's Group (06/2010)
- Academia: MIT crypto seminar (03/2009), Harvard colloquium (10/2009), UC San Diego (02/2011),
Technion colloquium (Haifa, Israel 05/2011)
- Workshops: DIMACS Secure Routing Workshop (New Brunswick, NJ, 03/2010)
ALIO-INFORMS session on "Routing and Incentives" (Buenos Aires, Argentina 06/2010)
- Industry: Representing the New England Research Lab at Microsoft's Techfest (Redmond, 03/2010)
BGPsec working group (Arlington, VA 04/2010), Cisco Tech Talk (San Jose 04/2010)

Measuring Loss and Delay in the Presence of Adversaries

- Industry: Microsoft Research ALT-TAB on Security (Redmond, WA 09/2009)

Securing Internet Routing

- Industry: Microsoft Research (Cambridge, MA 01/2009),
- Academia: MIT (02/2009), Boston University (02/2009), U Penn (02/2009), Georgia Tech (03/2009)

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), Northwestern (2/2010)

Path-Quality Monitoring in the Presence of Adversaries

- Conferences: ACM SIGMETRICS 2008 (Annapolis, MD, 06/2008)
- Industry: Microsoft Research (Cambridge, MA 01/2009),
Cisco (San Jose, CA, 03/2008)
- Academia: Georgia Tech (02/2009), New York University (12/2009), Weizmann Institute (Israel, 04/2008), Ben Gurion University (Be'er Sheva, Israel 04/2008), University of Toronto (09/2009), Brown University (11/2009)

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 Workshop on Hardware for Crypto (Los Angeles 12/2006)
- Industry: IBM Research (Hawthorne, NY, 01/2007) Telcordia (Red Bank, NJ, 03/2007)

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

CS 237 Probability in Computing , Boston University, Instructor	Spring 2011
CS 591 Seminar in Network Security , Boston University, Instructor	Fall 2010
ELE201 Intro to Electrical Signals & Systems , Princeton, Head Teaching Assistant	Spring 2006
ECE159 Fundamentals of Electricity & Circuits , University of Toronto, Tutor	Spring 2003
AER201 Engineering Design , University of Toronto, Extra-Help Tutor	Spring 2002

INTERNET STANDARDS

Invited Member, BGPsec informal design team	December 2009-Present
<ul style="list-style-type: none">Working with engineers and researchers from industry, government, and network operations, to design a new secure interdomain routing protocol prior to beginning formal proceedings within the IETF.	
Contributor, IETF PSAMP (Packet Sampling) Charter.	2007

WOMEN IN COMPUTER SCIENCE

WGBH Boston “Dot Divas”	2009-Present
<ul style="list-style-type: none">Participate in outreach events as part of an NSF-funded outreach program to interest girls in comp. sci.	
Graduate Women in Science and Engineering, (GWISE), Princeton University	
President (2007-2008), Vice-President (2006-2007), Secretary (2005-2006)	
<ul style="list-style-type: none">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
<ul style="list-style-type: none">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.	

ACADEMIC SERVICE : EXTERNAL

Program Committees:	NetEcon’11, SIGCOMM ’11, SIGCOMM’10 Student Poster Competition (Judge) CoNEXT Student Workshop ’11, USENIX HotCloud ’10, NetEcon ’10, NetEcon ’09
External Reviewer:	USENIX NSDI ’10, IACR EUROCRYPT ’10, 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.
Journal Reviewer:	IACR Journal of Cryptology, IEEE Trans. on Networking, IEEE Trans. on Communications, ACM Trans on Internet Technology, Journal of Knowledge and Information Systems