## Nadia Heninger


| | | |
|---|---|---|
| Contact Information | nadiah@cis.upenn.edu<br>http://www.cis.upenn.edu/~nadiah/ | +1 215-898-9252<br>Computer & Information Science Department<br>University of Pennsylvania<br>3330 Walnut St.<br>Philadelphia, PA 19104-3409 |


**Research Interests**

My research takes a mathematical approach to cryptography and systems security. I look for problems where mathematical or algorithmic tools can provide new insight on the security of real-world systems. Current areas of interest include cryptanalysis, computational number theory, network security, privacy, lattices, coding theory, and implications for public policy.

**Education**

May 2011, Ph.D. in computer science, **Princeton University**
Supervised by Bernard Chazelle.

Visiting graduate student in mathematics, **MIT**, September 2010–June 2011

Budapest Semesters in Mathematics, Spring 2005

December 2004, B.S. in electrical engineering and computer science with high honors, **University of California, Berkeley**

**Academic Positions Held**

July 2013–, Magerman Term Assistant Professor, University of Pennsylvania

July 2011–June 2012, NSF Mathematical Sciences Postdoctoral Research Fellow, University of California, San Diego

**Industrial Positions Held**

July 2012–June 2013, Visiting Researcher, Microsoft Research New England

June–September 2010, Intern, Microsoft Research New England

December 2009–March 2010, Intern, Microsoft Research New England

June–August 2005, Intern, AT&T Labs

January–August 2002, Intern, World Wide Web Consortium, INRIA Sophia-Antipolis

**Honors and Distinctions**

IRTF Applied Networking Research Prize, 2017

NSF CAREER Award, 2017

Best Paper Award, ACM CCS 2016

Pwnie Award - Best Cryptographic Attack, Black Hat 2016

Best Paper Award, ACM CCS 2015

Pwnie Award - Most Innovative Research, Black Hat 2015

Best Paper Award, USENIX Security 2012

NSF Mathematical Sciences Postdoctoral Research Fellowship, 2011–2013

Best Student Paper Award, USENIX Security 2008

Pwnie Award - Most Innovative Research, Black Hat 2008

National Science Foundation Graduate Research Fellowship, 2007–10

AT&T Labs Graduate Fellowship, 2005–07

Francis Lothrop Upton Fellowship, Princeton University, 2005

Ford Motor Company Scholarship, UC Berkeley, 2003–04

UC Berkeley EECS Honors Program

Eta Kappa Nu

## Publications in Refereed Journals

Yuval Yarom, Daniel Genkin, and Nadia Heninger. CacheBleed: A Timing Attack on OpenSSL Constant Time RSA. *Journal of Cryptographic Engineering* (2017) p. 1–14, 2017.

Henry Cohn and Nadia Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. *Advances in Mathematics of Communications* 9(3) p. 311-339, July 2015.

Henry Cohn and Nadia Heninger. Approximate common divisors via lattices. *Proceedings of the Tenth Algorithmic Number Theory Symposium* The Open Book Series 1(1) p. 271–293, November 2013.

J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: Cold boot attacks on encryption keys. *Communications of the ACM* 52(5):91–98, May 2009.

Nadia Heninger, Eric Rains and N. J. A. Sloane. On the integrality of $n$-th roots of generating functions. *Journal of Combinatorial Theory Series A* 113(8) p. 1732–1745, November 2006.

## Refereed Conference Proceedings

Daniel J. Bernstein, Joachim Breitner, Daniel Genkin, Leon Groot Bruinderink, Nadia Heninger, Tanja Lange, Christine van Vredendaal, and Yuval Yarom. Sliding right into disaster: Left-to-right sliding windows leak. *CHES 2017.* Taipei, Taiwan. September 25–28, 2017.

Daniel J. Bernstein, Nadia Heninger, Paul Lou, and Luke Valenta. Post-Quantum RSA. *PQCrypto 2017.*

Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thomé. A kilobit hidden SNFS discrete logarithm computation. *Eurocrypt 2017* Paris, France. June 1–3 2017.

Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. Alex Halderman, Nadia Heninger. Measuring small subgroup attacks on Diffie-Hellman. *Network and Distributed System Security Symposium* San Diego, California. February 27–March 1, 2017.

Ted Chinburg, Brett Hemenway, Nadia Heninger, and Zachary Scherr. Cryptographic applications of capacity theory: On the optimality of Coppersmith's method for univariate polynomials. *AsiaCrypt 2016.* Hanoi, Vietnam, December 5–8 2016.

Marcella Hastings, Joshua Fried, Nadia Heninger. Weak keys remain widespread in network devices. *Internet Measurement Conference* Santa Monica, CA, November 14–16 2016.

Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. A Systematic Analysis of the Juniper Dual EC Incident. *23rd ACM Conference on Computer and Communications Security.* Vienna, Austria, October 25–27 2016. **Best Paper Award.**

Yuval Yarom, Daniel Genkin, and Nadia Heninger. CacheBleed: A Timing Attack on OpenSSL Constant Time RSA. *Conference on Cryptographic Hardware and Embedded Systems*, Santa Barbara, California, August 17–19 2016.

D Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar, and Yuval Shavitt. ROWN: Breaking TLS using SSLv2.*25th Usenix Security Symposium*, Austin, Texas August 10–12 2016.

Luke Valenta, Shaanan Cohney, Alex Liao, Joshua Fried, Satya Bodduluri, and Nadia Heninger. Factoring as a Service. *20th International Conference on Financial Cryptography and Data Security*, Barbados February 22–26 2016.

David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. 13p. *22nd ACM Conference on Computer and Communications Security*, Denver, CO, October 12–15 2015. **Best paper award.**

Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow. Elliptic Curve Cryptography in Practice. 16p. *18th International Conference on Financial Cryptography and Data Security*, Barbados March 3–7 2014.

Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, and Nicko van Someren. Factoring RSA keys from certified smart cards: Coppersmith in the wild. 20p. *AsiaCrypt 2013*, Bangalore, India December 2–5 2013.

Deepika Gopal and Nadia Heninger. Torchestra: Reducing interactive traffic delays over Tor. 12p. Workshop on Privacy in the Electronic Society, Raleigh, NC, October 15, 2012.

Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. 16p. *21st USENIX Security Symposium*, Bellevue, WA August 8–10 2012. **Best paper award.**

Casey Devet, Ian Goldberg, and Nadia Heninger. Optimally robust private information retrieval. *21st USENIX Security Symposium*, Bellevue, WA August 8–10 2012.

Henry Cohn and Nadia Heninger. Approximate common divisors via lattices. 17p. *Tenth Algorithmic Number Theory Symposium*, San Diego, CA July 9–13 2012.

Henry Cohn and Nadia Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. 11p. *Proceedings of Innovations in Computer Science 2011*, Beijing, China January 7–9 2011.

Nadia Heninger. Computational complexity and information asymmetry in election audits with low-entropy randomness. *Electronic Voting Technology/Workshop on Trustworthy Elections 2010*, Washington, DC, August 9–10 2010.

Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, Emmett Witchel. Defeating Vanish with low-cost Sybil attacks against large DHTs. 17p. *17th Network and Distributed System Security Symposium*, San Diego, CA, March 1–3 2010.

Nadia Heninger and Hovav Shacham. Reconstructing RSA private keys from random key bits. 17p. *Crypto 2009*, Santa Barbara, CA, August 16–20 2009.

William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. Fingerprinting blank paper using commodity scanners. 14p. *30th IEEE Symposium on Security and Privacy*, Oakland, CA, May 17–20 2009.

J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: Cold boot attacks on encryption keys. 15p. *17th USENIX Security Symposium*, San Jose, CA, July 30–August 1 2008. **Best student paper award.**

OTHER

"Cold boot attacks" in van Tilborg, Henk C.A., Jajodia, Sushil (Eds.) *Encyclopedia of Cryptography and Security (2nd ed.)* Springer. 2011.

FUNDING

NSF CAREER: Cryptographic Security at Internet Scale
Awarded 7/2017

Cisco Equipment Gifts
Awarded 1/2016, 7/2016, and 7/2017

NSF TWC: Medium: Cryptographic Applications of Capacity Theory
Ted Chinburg, Brett Hemenway, Nadia Heninger co-PIs Awarded 10/2015

Amazon AWS Research Education Grant Awarded 6/2015 and 10/2015

Cisco: Security Protocol Analysis Cluster Engineering
Nadia Heninger and Jonathan Smith co-PIs Awarded 4/2015

Intel-NSF CPS: Synergy: Collaborative Research: Security and Privacy-Aware Cyber-Physical Systems, Lee, Haeberlen, Hanson, Heninger, Koppel, Pajic, Pappas, Phan, Sokolsky, Vagle, Yoo, Shin Awarded 5/2015

NSF TWC: Medium: Collaborative: Black-box evaluation of cryptographic entropy at scale J. Alex Halderman, Nadia Heninger, Hovav Shacham co-PIs Awarded 10/2014.

NSF Mathematical Sciences Postdoctoral Research Fellowship
Awarded 7/2011.

INVITED SEMINARS/LECTURES/PRESENTATIONS

*Adventures in RSA key recovery*
**Invited Lecture, Latincrypt** Havana, Cuba September 2017

*Factoring algorithms and lattice attacks against RSA*
Three hours of lectures at the IACR Advanced School of Cryptography, Havana, Cuba, September 2017

*A kilobit hidden SNFS discrete logarithm calculation*
Foundations of Computational Mathematics Number Theory Workshop, Barcelona, Spain, July 2017
Oberwolfach, Germany, January 2017

*Random number generation done wrong*
Wr0ng Workshop, Paris, May 2017

*How not to implement Diffie-Hellman*
CrossFyre Workshop, Paris, May 2017
ETH Zurich security seminar, March 2017

*The legacy of export-grade cryptography in the 21st century*
CMU Security seminar, January 2017
UIUC Security seminar, October 2016
Summer school on real-world crypto and privacy (with J. Alex Halderman), Sibenik, Croatia, June 2016
Security in Times of Surveillance workshop, Eindhoven, Netherlands, May 2016
IDA-CCR Princeton, April 2016

*The Reality of Cryptographic Deployments on the Internet*

**Invited lecture, AsiaCrypt**, Hanoi, Vietnam, December 2016

*Cryptographic applications of capacity theory*
Workshop on Mathematical Structures for Cryptography, Leiden, Netherlands, August 2016

*Cryptography is Hard*
Data and Society: Practice and Challenge, New York, May 2016

*How Diffie-Hellman fails in practice*
Cisco research seminar, November 2015
UPenn Security-Special Interest Group, October 2015
UPenn AMCS/PICS Colloquium, October 2015;
Elliptic Curve Cryptography Workshop, Bordeaux, France, October 2015
Simons Institute Workshop on The Mathematics of Modern Cryptography, Berkeley, CA, July 2015
DIAMANT Symposium, Netherlands, May 2015
Facebook Beers and Breakage Seminar, May 2015

*Factoring and discrete log algorithms*
School on Security of Cryptographic Algorithms and Devices for Real-World Applications, Sibenik, Croatia, June 2015

*Detection of widespread weak keys in network devices/*
*How not to generate random numbers*
School on Security of Cryptographic Algorithms and Devices for Real-World Applications, Sibenik, Croatia, June 2015
Stanford EE Colloquium, May 2015
**Five-hour invited tutorial** at CryptoAction School on Cryptographic Attacks, Porto, Portugal, October 2014
**Invited lecture**, International Conference on Applied Cryptography and Network Security **(ACNS)**, Lausanne, Switzerland, June 2014
Seminar, ENS Lyon, France, June 2014
Villanova CS Colloquium, April 2014
EPFL CS Colloquium, Switzerland, December 2013
UC Berkeley security seminar April 2013
**Invited lecture**, RSA Conference Cryptographer's Track **(CT-RSA)** San Francisco, CA, February 2013
Real-World Cryptography workshop, Stanford January 2013
MIT security seminar December 2012
Taiwan-Germany Workshop on Information Security and Cryptography (with J. Alex Halderman), National Chung-Hsing University, Taichung, Taiwan, November 2012
Aarhus University theory seminar November 2012
UCSD cryptography seminar April 2012
UC Irvine cryptography seminar March 2012

*Provably solving multivariate approximate common divisors via lattices*
ICERM Workshop on Mathematics of Lattices and Cybersecurity, Brown University, April 2015

*Black-Box Cryptanalysis*
ICERM Workshop on Mathematics of Cybersecurity, Brown University, October 2014

*Approximate common divisors via lattices*
Seminar, ENS Lyon, France, June 2014
Crypto Working Group seminar, Utrecht Netherlands, May 2014
Workshop on Lattice-Based Cryptography, Bangalore, India December 2013

Mathematical and Statistical Aspects of Cryptography, Calcutta, India January 2012
U Waterloo cryptography seminar December 2011
UC Irvine cryptography seminar November 2011

*Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding/ Lattices in cryptanalysis and list-decoding of error-correcting codes*
UPenn Mathematics Colloquium, February 2014
**Invited lecture**, Symbolic Computation and Cryptography **(SCC 2012)** Castro Urdiales, Spain July 2012;
SIAM Conference on Applied Algebraic Geometry, Raleigh, NC, October 2011
AWM 40 Years and Counting Conference, Providence, RI, September 2011
TU Eindhoven, March 2011
UC San Diego, February 2011
AT&T Labs, May 2010
Theory reading group Microsoft/MIT, February 2010

*Factoring made easy*
Microsoft Research New England 5th Anniversary Celebration, Cambridge, MA, October 2013

*Tutorial on lattice-based cryptography*
Dagstuhl Workshop on Quantum Cryptanalysis, Germany September 2013
Workshop on Post-Quantum Cryptography and Quantum Algorithms Leiden, Netherlands November 2012

*Polynomial versions of Coppersmith's Theorem*
SIAM Conference on Applied Algebraic Geometry, Fort Collins, CO, August 2013

*Adventures in public-key cryptanalysis*
**Four-hour invited tutorial** at Technion Summer School on Computer Security, Haifa, Israel, July 2013

*The state of factoring algorithms and other cryptanalytic threats to RSA*
ISAT workshop keynote (with Daniel J. Bernstein and Tanja Lange) January 2013

*Cryptanalysis and side-channel attacks*
Pomona College CS colloquium, September 2011

*Cold boot attacks against encryption keys*
TU Eindhoven, March 2011
Guest lecture in graduate network security course, Boston University, October 2010
MIT security seminar, September 2010
NY Area Crypto Day, April 2010
Workshop on Provable Security against Physical Attacks Leiden, Netherlands, February 2010
Confidence 2.0 Warsaw, Poland November 2009
AT&T Labs Seminar, May 2008
IDA-CCR Princeton Seminar, May 2008

*Reconstructing RSA private keys from random key bits*
AT&T Labs Seminar, May 2009
UC San Diego Seminar, March 2009
University of Michigan Theory Seminar, March 2009

*Fingerprinting blank paper using commodity scanners*
Security seminar, UC San Diego, March 2009

*If a power series were a power of a power series, what power would it be, seriously?*
AT&T Labs Seminar, August 2005

## Panels

*Restoring Personal Privacy without Compromising National Security* with Whit Diffie, Bryan Ford, Paul Syverson, and Joan Feigenbaum, San Francisco, May 2017

*Cybersecurity: Mathematics and Policy* with Susan Landau, Ron Rivest, and Alice Silverberg, American Association for the Advancement of Science Annual Meeting, Boston, February 2017

*Theory x Practice Driven Cryptography: Future Challenges and Opportunities* with Jeroen van de Graaf and Marcos Simplicio, Brazil-USA Workshop on Cybersecurity and Privacy on the Internet, Brasilia, Brazil, December 2015

*PETs Post-Snowden: Implications of the revelations of the NSA and GCHQ Surveillance Programs for the PETs community*
with Wendy Seltzer, Marek Tuszynski, George Danezis, and Seda Gurses, PET Symposium Amsterdam, Netherlands, July 2014

## Teaching

CIS 331 - Introduction to Networks and Computer Security, Fall 2017
CIS 331 - Introduction to Networks and Computer Security, Spring 2017
CIS 800 - Security Seminar, Spring 2017
CIS 556 - Cryptography, Fall 2016
CIS 800 - Security Seminar, Fall 2016
CIS 331 - Introduction to Networks and Computer Security, Spring 2016
CIS 800 - Security Seminar, Spring 2016
CIS 556 - Cryptography, Fall 2015
CIS 800 - Security Seminar, Fall 2015
CIS 331 - Introduction to Networks and Computer Security, Spring 2015
CIS 800 - Security Reading Group, Spring 2015
Preceptorial - Security for the Curious, Fall 2014
CIS 700 - Cryptography, Fall 2014
CIS 800 - Security Reading Group, Fall 2014
CIS 331 - Introduction to Networks and Computer Security, Spring 2014
CIS 800/02 Topics in Cryptography, Fall 2013

## Advising

*Postdocs*
Barak Shani fall 2017–
Daniel Genkin (co-advised with Jonathan Katz) fall 2016–

*PhD students*
Jan Henrik Wiik (AMCS, anticipated 2022)
Gabrielle De Micheli (CIS, anticipated 2021)
Marcella Hastings (CIS, anticipated 2020)
Shaanan Cohney (CIS, anticipated 2019),
Luke Valenta (CIS, anticipated 2019)

*PhD committees*
Laurent Grémy (CS, Université de Lorraine, France, September 2017)
Christina Garman (CS, Johns Hopkins, August 2017)
Vincent Neiger (Math, ENS de Lyon, France, November 2016)
Sandy Clark (CIS, October 2016)
Cyril Bouvier (Math, Université de Lorraine, France, July 2015)
Edvard Fagerholm (Math, April 2015)
Dong Lin (CIS, March 2015)

*Masters projects supervised*
B. B. de Kock (visiting student from TU Eindhoven, spring 2017)
Richard Roberts (CIS masters thesis spring 2016)
Michael Rudow (Math masters thesis spring 2016)

Joshua Fried (Independent study spring 2016, summer 2017)
Eitan Goldberger (Independent study summer 2015)
Dennis Sell (Independent study spring 2015)
Leon Groot Bruinderink (visiting student from TU Eindhoven, Fall 2014)
Shruthi Gorantala (Independent study 2014–2015)
Deepika Gopal (UCSD, spring 2012)

*Undergraduate projects supervised*
Lauren Leung (Independent study fall 2017)
Paul Lou (CIS 400 fall 2017, Rachleff scholar summer 2016)
Henry Zhu (PURM undergraduate researcher, summer 2017)
Jeff Barg and Ajay Patel (CIS 400, spring 2017)
Tom Yurek (Research assistant summer 2016, visiting from Purdue)
Joseph Cappadona (Research assistant summer 2016)
Terry Sun (Independent study spring 2015, spring 2016, RA summer 2016)
Richard Roberts (Independent study spring 2015, spring 2016)
Michael Rudow (Independent study spring 2016, fall 2016)
Sudarshan Muralidhar, Doron Shapiro, Michelle Socher (CIS 400, fall 2015–spring 2016, 1st place in department competition)
Justin MacIntosh and Richard Roberts (CIS 400, fall 2015–spring 2016, 3rd place in department competition)
Alex Liao (Research assistant summer 2015)
Joseph Ooi (EAS 499, spring 2015)
Darren Yin (Independent study spring 2015)
Jerry Guo (EAS 499, spring 2014)
Starry Peng (EAS 499, fall 2013)

## Service

*Program chair*
2019 Usenix Security Symposium

*Program committees*
2018 Usenix Security Symposium
2018 IEEE Security and Privacy
2017 Real World Crypto
2017 Usenix Security Symposium
Crypto 2017: International Cryptology Conference
2016 Usenix Security Symposium
2016 ArticCrypt
2016 IEEE Security and Privacy
2016 Privacy Enhancing Technologies Symposium
2015 Usenix Security Symposium
2015 IEEE Security and Privacy
2015 Financial Cryptography
2014 Usenix Security Symposium
Crypto 2014: International Cryptology Conference
2014 Award for Outstanding Research in Privacy-Enhancing Technologies
2014 Workshop on the Economics of Information Security
2014 International Conference on Post-Quantum Cryptography
LatinCrypt 2014: International Conference on Cryptology and Information Security in Latin America
PKC 2014: International Conference on Practice and Theory of Public-Key Cryptography
2011 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections

*Funding Review Panels*

Open Technology Fund Advisory Council 2014–
2014 NSF SaTC review panel

*External reviewing*

CCS 2017, ANTS 2016, Crypto 2015, Asiacrypt 2013, CCS 2013, SAC 2013, Crypto 2013, Asiacrypt 2012, PKC 2012, Journal of Cryptography, Designs, Codes, and Cryptography, Financial Cryptography 2012, Journal of Cryptographic Engineering, CT-RSA 2012, SODA 2012, Oakland 2011, TCC 2011, Indocrypt 2010, CCS 2010, EVT/WOTE 2010, Crypto 2010, SAC 2009, CCS 2009

*Steering committee*

NDSS, 2017–

*Outreach*

"Picking Research Problems" panelist with Franzi Roesner at GREPSEC 2017
"Perception and (un)equal opportunities for women" panelist at CrossFyre Workshop, May 2017
Organizing committee, GREPSEC 2017
"So You Want to Hack The Planet: Demystifying Careers and Opportunities in Cryptography, Security & Privacy" panelist at Grace Hopper, October 2016
"Choosing the right research direction" panelist with Susan Landau, GREPSEC Workshop for women and underrepresented women in security, San Jose, CA, May 2015
Presented at Mini Women in CS HS Day, November 2014
Presented at Camp Women in CS, UPenn, March 2014
Team leader, OurCS Workshop for Undergraduate Women in CS, CMU, October 2013
Team leader, OurCS Workshop for Undergraduate Women in CS, CMU, March 2011
Mentor for Summer Programming Experience program for undergraduates, Princeton University, Summer 2009

*University Speaking*

Research overview presentation, PhD student open house, March 2016
Research overview presentation, prospective PhD student open house, November 2015
Presented on "Information Security, Privacy, and Data Integrity" at Responsible Conduct of Research workshop, UPenn, April 2015
Panelist for "Studying for the PhD event" in UPenn CIS, February 2015
Speaker for Center for Teaching and Learning graduate workshop, September 2014
"Cryptography, security, and you" invited lecture at Philomathean Society, UPenn, April 2014

*Department WPE II committees*

Kevin Tian (Spring 2015, chair)
Perry Metzger (Fall 2013)

*Department Seminars*

Restarted and co-organized weekly UPenn CS theory seminar Fall 2013–Spring 2014 with Aaron Roth

## Other

*Policy*

"Chilling effects of the DMCA on security research" Congressional briefing with Matthew Green, Jen Ellis, Dan Nabel, Jonathan Band, Washington DC, May 2015
2015 DMCA Exemption Submission for Software-Security Research, with Matt Blaze, J. Alex Halderman, Ed Felten, and Steve Bellovin

*Popularization*

"Logjam: Diffie-Hellman, discrete logs, the NSA, and you" presentation at 32C3 with J. Alex Halderman, Hamburg, Germany, December 2015

"How is NSA breaking so much crypto?" blog post with J. Alex Halderman, Freedom to Tinker, October 2015

"Crypto Tales from the Trenches" Organized panel with Julia Angwin, Laura Poitras, and Jack Gillum at 31C3, Hamburg, Germany, December 2014

"The year in crypto" presentation at 30C3 with Daniel J. Bernstein and Tanja Lange Hamburg, Germany December 2013

"Tales from the crypto community" with J. Alex Halderman *Foreign Affairs* online October 23, 2013.

"RSA factorization in the real world" presentation at 29C3 with Daniel J. Bernstein and Tanja Lange Hamburg, Germany December 2012

"New research: There's no need to panic over factorable keys–just mind your Ps and Qs" blog post at Freedom to Tinker, February 2012

*Selected Media Coverage*

"Why quantum computers might not break cryptography"
Quanta Magazine 5/2017

"Des nombres truqués pour mieux espionner"
Le Monde 10/2016

"Drown attack: How weakened encryption jeopardizes 'secure' sites"
The Guardian 3/2016

"Breaking 512-bit RSA with Amazon EC2 is a cinch. So why all the weak keys?"
Ars Technica 10/2015

"Could a simple mistake be how the NSA was able to crack so much encryption?"
The Guardian 10/2015

"New Computer Bug Exposes Broad Security Flaws"
Wall Street Journal 5/2015

"LogJam: Sicherheitslücke bei verschlüsselten Verbindungen - so schützen Sie sich"
Der Spiegel 5/2015

"FREAK flaw undermines security for Apple and Google users, researchers discover"
Washington Post 3/2015

"Fatal crypto flaw in some government-certified smartcards makes forgery a snap"
Ars Technica 9/2013

"Crypto shocker: four of every 1,000 public keys provide no security"
Ars Technica 2/2012

"Researchers Find Way to Steal Encrypted Data"
NY Times 2/2008

MISC US Citizen