

Nadia Heninger

CONTACT INFORMATION nadiah@cs.ucsd.edu
<http://www.cs.ucsd.edu/~naheninger/>

RESEARCH INTERESTS Algorithms. The mathematics of cryptography, particularly cryptanalysis of RSA. Using tools from theoretical computer science to model real-world problems. Applications to security and policy.

EDUCATION Ph.D. in computer science, **Princeton University**, May 2011
 Supervised by Bernard Chazelle.
 Visiting graduate student in mathematics, **MIT**, September 2010–June 2011
 Budapest Semesters in Mathematics, Spring 2005
 B.S. in electrical engineering and computer science with high honors,
 University of California, Berkeley, 2004

AWARDS AND HONORS 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

EMPLOYMENT NSF Mathematical Sciences Postdoctoral Research Fellow
 University of California, San Diego, La Jolla, CA, July 2011–
 Intern
 Microsoft Research New England, Cambridge, MA, June–September 2010
 Intern
 Microsoft Research New England, Cambridge, MA, December 2009–March 2010
 Intern
 AT&T Labs Florham Park, NJ, June–August 2005
 Research Experience for Undergraduates
 East Tennessee State University, June–August 2004
 Intern
 World Wide Web Consortium, INRIA Sophia-Antipolis, France, January–August 2002

TEACHING Mentor for Summer Programming Experience program for undergraduates
 Princeton University, Summer 2009
 Teaching Assistant, Algorithms and Data Structures
 Princeton University, Spring 2008
 Teaching Assistant, General Computer Science
 Princeton University, Fall 2006

PAPERS

- Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. Henry Cohn and Nadia Heninger. *Proceedings of Innovations in Computer Science 2011*, January 2011
- Computational complexity and information asymmetry in election audits with low-entropy randomness. Nadia Heninger. *Proceedings of EVT/WOTE 2010*, August 2010
- Defeating Vanish with low-cost Sybil attacks against large DHTs. Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, Emmett Witchel. *Proceedings of the 17th Network and Distributed System Security Symposium*, San Diego, CA, February–March 2010
- Reconstructing RSA private keys from random key bits. Nadia Heninger and Hovav Shacham. *Proceedings of Crypto 2009*, vol. 5677 of LNCS. p. 1–17. Springer-Verlag. Santa Barbara, CA, August 2009
- Fingerprinting blank paper using commodity scanners. William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, p. 301–314, Oakland, CA, May 2009
- Lest we remember: Cold boot attacks on encryption keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. *Proceedings of the 17th USENIX Security Symposium*, p. 45–60, San Jose, CA, July–August 2008. Reprinted in *Communications of the ACM* 52(5):91–98, May 2009
- On the integrality of n -th roots of generating functions. Nadia Heninger, Eric Rains and N. J. A. Sloane. *Journal of Combinatorial Theory Series A* Volume 113, Issue 8 (November 2006) p. 1732–1745
- Upper bounds on graph integrity and vertex-neighbor-integrity. Nadia Heninger, Anne Shiu, and Annalies Vuong. Manuscript, 2004

TALKS

- How the cryptanalysis of RSA is (not so) secretly coding theory*
UC San Diego, February 2011; TU Eindhoven, March 2011
- Lest we remember: Cold boot attacks against encryption keys*
Guest lecture in graduate network security course, Boston University, October 2010; TU Eindhoven, March 2011
- Recovering cryptographic keys with the cold boot attack*
Systems security reading group, MIT, September 2010
- Mathematics and side-channel attacks*
Presentation for thesis committee at Princeton, May 2010
- How the cryptanalysis of RSA is (not so) secretly coding theory*
AT&T Labs, May 2010
- Recovering cryptographic keys with the cold boot attack*
Workshop on Provable Security against Physical Attacks Leiden, Netherlands, February 2010; NY Area Crypto Day, April 2010
- Coppersmith's theorem and list-decoding of Reed-Solomon codes.*
Reading group Microsoft/MIT, February 2010
- Practical information on the cold boot attack.*
Confidence 2.0 Warsaw, Poland November 2009

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

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

Recovering cryptographic keys from memory images
AT&T Labs, May 2008; IDA-CCR Princeton, May 2008

Minimum spanning trees of random subgraphs
Presentation for general exam, Princeton, May 2007

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

Classes of graphs with bounded integrity
Big Sky Conference on Discrete Mathematics, University of Montana-Missoula, September 2004; AMS/MAA Joint Meetings, Atlanta, January 2005

SERVICE

Program Committee for EVT/WOTE 2011

External reviewer for Oakland 2011, TCC 2011, Indocrypt 2010, CCS 2010, EVT/WOTE 2010, Crypto 2010, SAC 2009, CCS 2009

Team leader for OurCS Workshop for Undergraduate Women in CS, March 2011

MISCELLANY

American citizen

Python, Perl, C, C++, Java, Lisp, Matlab, Mathematica

Proficient in French, elementary knowledge of Norwegian, German, and Hungarian, coursework in Russian and Chinese