

JOSHUA A. KROLL

94 Spring Grove Avenue, San Anselmo, CA 94960

(831) 521-2260 • jkroll@jkroll.com

EDUCATION

Princeton University Princeton, NJ • PhD (2015): Computer Science

Dissertation: *Accountable Algorithms*

Advisors: Edward W. Felten and Andrew Appel

Summary: Relating trust and assurance in computer science to oversight and accountability in public policy, including a novel cryptographic approach to using the tools of the first to enable the second.

Princeton University Princeton, NJ • MA (2011): Computer Science

General Exam Title: "Portable, Verifiable Low-Level Memory Safety"

Harvard College Cambridge, MA • AB (2009): Physics and Mathematics. Secondary Field: Computer Science

John Wood Science Prize, Adams House Arms

PUBLICATIONS

PEER-REVIEWED

- **Kroll, J. A.**, J. Huey, S. Barocas, E. W. Felten, J. Reidenberg, D. Robinson, and H. Yu. "Accountable Algorithms". *University of Pennsylvania Law Journal*, Vol. 165, Issue 3. 2016. *Future of Privacy Forum Privacy Papers for Policymakers Award, 2016*
- Bonneau, J., A. Miller, J. Clark, A. Narayanan, **J. A. Kroll**, and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", 36th IEEE Symposium on Security and Privacy, San Jose, CA, May 2015.
- **Kroll, J. A.**, E. W. Felten, and J. A. Haldermann, "Efficiently Auditing Multi-Level Elections", 6th International Conference on Electronic Voting, October, 2014.
- A. Edmundsen, A. K. Simpson, **J. A. Kroll**, and E. W. Felten, "Security Audit of Safeplug 'Tor in a Box'", 4th USENIX Workshop on Free and Open Communication on the Internet, August, 2014.
- **Kroll, J. A.**, J. Stewart, and A. Appel "Portable Software Fault Isolation", Computer Security Foundations, July 2014.
- Clark, J., J. Bonneau, E. W. Felten, **J. A. Kroll**, A. Miller, and A. Narayanan, "On Decentralizing Prediction Markets and Order Books", Workshop on the Economics of Information Security, June 2014.
- Bonneau, J., A. Narayanan, A. Miller, J. Clark, **J. A. Kroll**, and E. W. Felten "Mixcoin: Anonymity for Bitcoin with accountable mixes", Financial Cryptography, March 2014.
- **Kroll, J. A.**, I. Davey and E. W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", Workshop on the Economics of Information Security, June 2013.
- **Kroll, J. A.** and D. Dean, "BakerSFeld: Bringing Software Fault Isolation to the x64", SRI Computer Science Laboratory Technical Report, 2009.
- Martell, C. and **J. A. Kroll**, "Corpus-Based Gesture Analysis: An extension of the FORM dataset for the automatic detection of phases in a gesture", *Int. J. Semantic Computing*, 1(4): 521-536 (2007).
- Martell, C. and **J. A. Kroll**, "Using FORM to Predict Phase Labels", *Proceedings of the Language Resources and Evaluation Conference, Workshop on Multimodal Corpora*, June 2006.

BOOK CHAPTERS

- **Kroll, J. A.**, I. Davey, and E. W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", *Economics of Information Security and Privacy*, Springer 2015.

OTHER

- **Kroll, J. A.**, "Accountable Algorithms". *PhD Dissertation*, Princeton University, August 2015.
- **Kroll, J. A.**, "The Cyber Conundrum", *The American Prospect*, Vol 26, No. 2. Spring 2015.
- **Kroll, J. A.**, "The Cyber Conundrum: A security update", *The American Prospect Online* June 3, 2015, <http://prospect.org/article/cyber-conundrum-security-update>

- Goldfeder, S., R. Gennaro, H. Kalodner, J. Bonneau, **J. A. Kroll**, E. W. Felten, and A. Narayanan, “Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme,” Manuscript. March, 2015.
- Barocas, S., E. W. Felten, J. Huey, **J.A. Kroll**, and A. Narayanan, “Big Data and Consumer Privacy in the Internet Economy”. Comment to the NTIA Big Data Request for Comments, 79 Fed. Reg. 32714. August 5, 2014.
- E. W. Felten and **J. A. Kroll**, “Heartbleed Shows Government Must Lead on Internet Security”, Scientific American, April 16, 2014, <http://www.scientificamerican.com/article/heartbleed-shows-government-must-lead-on-internet-security/>.
- **Kroll, J. A.**, E. W. Felten, and D. Boneh, “Secure Protocols for Accountable Warrant Execution,” Manuscript. April, 2014.

WORK HISTORY

CloudFlare, Inc. (August 2015-Present)

Systems Engineer (Software Engineer, Security Team)

- Developed and launched “Origin CA”, a Go microservice to sign TLS certificates for customer origin servers using CloudFlare-trusted certificates.
- Designed, implemented, and deployed PAL, a container identity attestation and secrets management system for Docker based on cryptographic access control via CloudFlare’s Red October.

Princeton University (2009-2015)

Graduate Research Fellow/PhD Candidate

- PhD research under Edward W. Felten and Andrew Appel. Work on accountable algorithms, cryptography, Bitcoin, electronic voting
- 9 peer reviewed papers. 1 law review article. 2 regulatory filings. 3 magazine articles. 1 book chapter. 8 invited talks.
- NSF Graduate Research Fellowship. Competitive award carrying university prize. 2000 given nationally.
- Press mentions: WIRED, MIT Technology Review, New Scientist, Scientific American

Elysium Digital, LLC (2014-2015)

Computer Scientist

- Litigation support consulting, focusing on intellectual property (patent, trademark) issues.

Google, Inc. (Summer 2012)

Intern, Engineering

- Worked on driver sandboxing and kernel-level memory integrity in Linux on the ChromeOS security team.

Google, Inc. (Summer 2011)

Intern, Engineering

- Worked on infrastructure-level projects involving security and privacy.

Google, Inc. (Summer 2010)

Intern, Public Policy Group

- Provided technical assessment of product privacy issues with legal and policy implications.

SRI International (Summer 2008, 2009)

Student Associate, Computer Science Lab

- Research in software-based containment solutions (“Sandboxing”) for 64-bit x86 architectures, pairing-based cryptography, and formal systems analysis.

Akamai Technologies, Inc. (June 2007-June 2008)
Software Engineering Intern, Mapping Division

- Designed & developed tools to monitor health/performance of the worldwide Domain Name System (DNS). Evaluated performance, failure modes, and security of common client-side DNS software.

Monterey Bay Aquarium Research Institute (Summer 2006)
Intern, Software Engineering

- Designed, implemented, and tested automated image classification unit for a computer vision system.

Naval Postgraduate School - Department of Computer Science (June 2004-August 2005)
Research Intern

- Performed research in Artificial Intelligence/Natural Language Processing as applied to human gestures.

Monterey Bay Aquarium (June 2001-August 2006)
Volunteer Guide

- Educated visitors as docent, presenter (6-7 shows/month; audiences of 150-450). Mentor and Tour Guide Certifications; 1000-Hour Service Award.

HONORS AND AWARDS

- Future of Privacy Forum Privacy Papers for Policymakers award, 2016
- National Science Foundation Graduate Research Fellowship (Award: 2011-2014; Honorable Mention: 2010)
- Member, NSF CISE Pathways to Revitalized Undergraduate Computing Education (CPATH) Rebooting Computing Summit Design Committee (Peter J. Denning, Chair) (2008-2009).

TEACHING

GRADUATE

- Princeton University, Department of Computer Science. Assistant in Instruction, Computer Science 226: Algorithms and Data Structures. Professor Robert Sedgewick, Instructor. Spring 2011.
- Princeton University, Department of Computer Science. Assistant in Instruction, Computer Science 432: Information Security. Professor Edward Felten, Instructor. Fall 2010.

UNDERGRADUATE

- Harvard University, Department of Mathematics. Head Course Assistant (of 6), Mathematics 23a/b: Linear Algebra and Real Analysis I/II. Dr. Paul G. Bamberg, Instructor. 2006-2007.

PRESENTATIONS

- **Kroll, J. A.** and Steven Roosa, “The Algorithm Made Me Do It: Predictive Power, Ethics and the Law in the Age of Machine Learning, Artificial Intelligence, and Mathematical Perplexity,” Highmark Health All-Hands Privacy Workshop, Pittsburgh, PA, January 11, 2017 (Invited).
- **Kroll, J. A.**, J. Huey, S. Barocas, E. W. Felten, J. Reidenberg, D. Robinson, and H. Yu, “Accountable Algorithms,” Workshop on Data and Algorithmic Transparency. NYU Law School. November 19, 2016. (*Selected by peer review*)
- **Kroll, J. A.** “Accountable Algorithms,” SRI International Computer Science Lab Formal Topics Seminar, Menlo Park, CA, October 19, 2016. (*Invited*)
- **Kroll, J. A.** and A. Powell, “Algorithmic Accountability,” Big Boulder Conference, Boulder, CO, June 24, 2016 (Invited).
- **Kroll, J. A.** “Accountable Algorithms,” Yale Law School Information Society Project Workshop on Unlocking the Black Box. April 1, 2016. (Selected by competitive review)
- **Kroll, J. A.**, “Accountable Algorithms,” London School of Economics Media Policy Project Workshop on Algorithmic Power in Black-Box Platforms, London School of Economics, January 25, 2016. (Invited)
- **Kroll, J. A.**, “Accountable Algorithms,” Princeton Center for Information Technology Policy and University of Vienna Media Innovation Lab Doctoral Workshop, Princeton University, April 8, 2015. (Selected by competitive review)

- **Kroll, J. A.**, “Accountable Algorithms,” Center for Information Technology Policy Luncheon Series, Princeton University, February 17, 2015.
- Felten, E. W. and **J. A. Kroll**, “Accountable Algorithms,” Fairness, Accountability, and Transparency in Machine Learning Workshop, Neural Information Processing Systems Conference, Montreal, Quebec, Canada, December 12, 2014. (Invited)
- **Kroll, J. A.**, “Big Data, Fairness, and Nondiscrimination”. New Jersey Attorney General’s Advocacy Institute In-Service Training, August 7, 2014.
- **Kroll, J. A.**, “Accountable Algorithms,” Princeton Joint ACM/IEEE Professional Society Chapter Meeting, April 17, 2014.
- **Kroll, J. A.**, “The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries,” Center For Information Technology Policy Luncheon Series, Princeton University, November 14, 2013.
- **Kroll, J. A.**, and G. Barber, “Drones: Not Just for Military Use,” New Jersey Attorney General’s Advocacy Institute In-Service Training, August 8, 2013 (CLE credit course).
- **Kroll, J. A.**, and E. W. Felten, “The State of Electronic Voting,” Center For Information Technology Policy Luncheon Series, Princeton University, October 18, 2012.
- **Kroll, J. A.**, “Seeing Under Sea: Applications of Computer Vision in Underwater Video,” *Plenary Address*, Harvard Undergraduate Research Symposium, Nov. 2006 (Accepted by faculty review; top 3 of 140 papers).

PROFESSIONAL SERVICE

- Program Chair, Workshop on Fairness, Accountability, and Transparency in Machine Learning (FATML’17)
- Organizer, Workshop on Fairness, Accountability, and Transparency in Machine Learning (FATML’16)
- External Reviewer, Journal of Big Data Special Issue on Social and Technical Trade-Offs
- Organizer, Workshop on Fairness, Accountability, and Transparency in Machine Learning (FATML’15)
- Technical Program Committee, 2015 Workshop on Fairness, Accountability, and Transparency in Machine Learning (FATML’15)
- Technical Program Committee, 2015 Workshop on Surveillance and Technology (SAT’15)
- Technical Program Committee, 2015 Workshop on Bitcoin Research (BITCOIN’15)
- Technical Program Committee, 2014 Workshop on Bitcoin Research (BITCOIN’14)
- External Reviewer, 2014 International Conference on Financial Cryptography and Data Security (FC’14)
- Member, Princeton University Faculty-Student Committee on Discipline (2011-2014)
- Member, Judicial Committee, Committee of the Princeton University Community (2010-2011)
- Student member (2009), Harvard Faculty of Arts and Sciences Committee on Information Technology