Ariel J. Feldman

Software Engineer
Google

111 8th Ave.
New York, NY 10011
ari@arifeldman.com
https://arifeldman.com

About me

I'm a software engineer at Google working on cloud key management and trusted execution environments. I work on systems security, especially on enabling users to outsource computation and sensitive data to third parties without having to fully trust them. I'm particularly interested in problems that intersect with law and public policy, such as electronic voting security, which has been the subject of some of my prior work.

Positions

10/18–present	**Google** (New York, NY). *Software Engineer*.
7/14–6/18	**University of Chicago, Dept. of Computer Science** (Chicago, IL). *Assistant Professor*.
7/12–6/14	**University of Pennsylvania, CIS Dept.** (Philadelphia, PA). *Postdoctoral Researcher*.
6/09–8/09	**United States Federal Trade Commission** (Washington, DC). *Intern*.
6/08–9/08	**Microsoft Research** (Redmond, WA). *Intern, Mentor: Josh Benaloh*.
6/07–8/07	**Google** (New York, NY). *Intern, Mentor: Umesh Shankar*.
9/04–6/05	**Brennan Center for Justice, NYU School of Law** (New York, NY). *Intern*.
8/03–9/04	**BAE Systems CNIR** (Wayne, NJ). *Software Engineer*.

Education

Princeton University ..... Princeton, NJ

Ph.D. in Computer Science ..... Jun. 2012
Advisor: Edward W. Felten
Thesis: *Privacy and Integrity in the Untrusted Cloud*
Committee: Andrew W. Appel, Michael J. Freedman, Brian W. Kernighan, David Walker

Brown University ..... Providence, RI

A.B. in Computer Science, A.B. in Philosophy; *magna cum laude* ..... May 2003
G.P.A.: 4.0/4.0

Honors and awards

Google Faculty Award (2016)

Best Student Paper, USENIX Security Symposium (2008 and 2012)

Princeton University: Upton Fellowship (2005)

Brown University: Ducasse Premium (2002), Phi Beta Kappa (2002), Sigma Xi (2003)

Refereed publications

[1] Min Xu, Antonis Papadimitriou, **Ariel J. Feldman**, and Andreas Haeberlen. Using Differential Privacy to Efficiently Mitigate Side Channels in Distributed Analytics. In *Proc. 11th European Workshop on Systems Security (Eurosec '18)*, March 2018.

[2] Bernard Dickens III, Haryadi S. Gunawi, **Ariel J. Feldman**, and Henry Hoffmann. StrongBox: Confidentiality, Integrity, and Performance using Stream Ciphers for Full Drive Encryption. In *Proc. 23rd ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '18)*, March 2018.

[3] Zhaoxia Deng, **Ariel J. Feldman**, Stuart A. Kurtz, and Frederic T. Chong. Lemonade from Lemons: Harnessing Device Wearout to Create Limited-Use Security Architectures. In *Proc. 44th International Symposium on Computer Architecture (ISCA '17)*, June 2017.

[4] Arjun Narayan, **Ariel J. Feldman**, Antonis Papadimitriou, and Andreas Haeberlen. Verifiable Differential Privacy. In *Proc. 2015 European Conference on Computer Systems (EuroSys '15)*, April 2015.

[5] Benjamin Braun, **Ariel J. Feldman**, Zuocheng Ren, Srinath Setty, Andrew J. Blumberg, and Michael Walfish. Verifying Computations with State. In *Proc. 24th ACM Symposium on Operating Systems Principles (SOSP '13)*, November 2013.

[6] **Ariel J. Feldman**, Aaron Blankstein, Michael J. Freedman, and Edward W. Felten. Social Networking with Frientegrity: Privacy and Integrity with an Untrusted Provider. In *Proc. 21st USENIX Security Symposium (Sec '12)*, Bellevue, WA, August 2012. **Awarded Best Student Paper**.

[7] **Ariel J. Feldman**, William P. Zeller, Michael J. Freedman, and Edward W. Felten. SPORC: Group Collaboration using Untrusted Cloud Resources. In *Proc. 9th Symposium on Operating Systems Design and Implementation (OSDI '10)*, October 2010.

[8] **Ariel J. Feldman** and Josh Benaloh. On Subliminal Channels in Encrypt-on-Cast Voting Systems. In *Proc. 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop (EVT/WOTE '09)*, August 2009.

[9] Stephen Checkoway, **Ariel J. Feldman**, Brian Kantor, J. Alex Halderman, Edward W. Felten, and Hovav Shacham. Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage. In *Proc. 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop (EVT/WOTE '09)*, August 2009.

[10] 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. In *Proc. 17th USENIX Security Symposium (Sec '08)*, July 2008. **Awarded Best Student Paper**.

[11] **Ariel J. Feldman**, J. Alex Halderman, and Edward W. Felten. Security Analysis of the Diebold AccuVote-TS Voting Machine. In *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*, August 2007.

Invited publications, technical reports, and other publications

[12] **Ariel J. Feldman**, Aaron Blankstein, Michael J. Freedman, and Edward W. Felten. Privacy and Integrity are Possible in the Untrusted Cloud. In *IEEE Data Engineering Bulletin*, December 2012.

[13] **Ariel J. Feldman**. *Privacy and Integrity in the Untrusted Cloud*. PhD thesis, Princeton University, 2012.

[14] 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.

[15] J. Alex Halderman and **Ariel J. Feldman**. AVC Advantage: Hardware Functional Specifications. Technical Report TR-816-08, Princeton University, Department of Computer Science, March 2008.

[16] Joseph A. Calandrino, **Ariel J. Feldman**, J. Alex Halderman, David Wagner, Harlan Yu, and William P. Zeller. Source Code Review of the Diebold Voting System. Part of the California Secretary of State's "Top-to-Bottom" Voting Systems Review, July 2007.

[17] Marjorie Heins, Christina Cho, and **Ariel Feldman**. Internet Filters: A Public Policy Report, Second Edition. Brennan Center for Justice at NYU School of Law, Free Expression Policy Project, May 2006.

Invited talks and refereed conference and workshop presentations

Higher Ed Security: A Researcher's Perspective

NACUBO Higher Education Accounting Forum, May 9, 2017

Verifying Computations with (Private) State

Purdue CERIAS, Nov. 11, 2015

Argonne National Laboratory, Aug. 4, 2015

DePaul CDM, May 8, 2015

Verifiable Differential Privacy

Greater Chicago Area Systems Research Workshop, Chicago, IL, Apr. 27, 2015

Designing Systems for Skeptics

USC, Apr. 24, 2014

Drexel University, Apr. 21, 2014

Google, Inc., Apr. 4, 2014

CMU, Mar. 26, 2014

University of Chicago, Mar. 3, 2014

NYU School of Engineering, Feb. 27, 2014

Social Networking with Frientegrity: Privacy and Integrity with an Untrusted Provider

21st USENIX Security Symposium, Bellevue, WA, Aug. 10, 2012

Privacy and Integrity in the Untrusted Cloud

Yale University, May 10, 2012

University of Pennsylvania, May 4, 2012

Columbia University, Mar. 20, 2012

MIT, Feb. 27, 2012

SPORC: Group Collaboration using Untrusted Cloud Resources

DIMACS Workshop on Cloud Computing, Newark, NJ, Dec., 9, 2011

Google, Inc., New York, NY, Dec. 15, 2010

9th Symposium on Operating Systems Design and Implementation, Vancouver, BC, Oct. 5, 2010

IBM Research Student Workshop for Frontiers of Cloud Computing, Hawthorne, NY, Sep. 10, 2010

On Subliminal Channels in Encrypt-on-Cast Voting Systems

USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop, Montreal, QC, Aug. 11, 2009

Security Analysis of the Diebold AccuVote-TS Voting Machine

USENIX/ACCURATE Electronic Voting Technology Workshop, Boston, MA, Aug. 6, 2007

Teaching

Spring 2018	CMSC 33251: Topics in Computer Security: Cloud and Distributed Systems Security (University of Chicago)
Winter 2018	CMSC 15200: Introduction to Computer Science II (University of Chicago)
Fall 2017	CMSC 23200/33250: Introduction to Computer Security (University of Chicago)
Winter 2017	CMSC 33251: Topics in Computer Security: Cloud and Distributed Systems Security (University of Chicago)
Spring 2016	CMSC 33251: Topics in Computer Security: Cloud and Distributed Systems Security (University of Chicago)
Winter 2016	CMSC 23200/33250: Introduction to Computer Security (University of Chicago)
Fall 2015	CMSC 23200/33250: Introduction to Computer Security (University of Chicago)
Spring 2015	CMSC 33251: Topics in Computer Security: Cloud and Distributed Systems Security (University of Chicago)
Winter 2015	CMSC 16200: Honors Introduction to Programming, II (University of Chicago)
Fall 2014	CMSC 23200/33250: Introduction to Computer Security (University of Chicago)
Spring 2007	COS 116: The Computational Universe (Princeton), *Assistant in Instruction*
Fall 2007	COS 126: General Computer Science (Princeton), *Assistant in Instruction*

Advising and mentoring

Graduate students

Galen Harrison (Ph.D. in progress; advised during M.S.)

Min Xu (Ph.D. 2020; advised during M.S.)

Minhaj Us Salam Khan (M.S. 2019)

Sotiri Komissopoulos (B.S./M.S. 2017)

Austin Byers (B.S./M.S. 2016)

Undergraduate independent work

Nathaniel Verhaaren (2018)

Julia Xu (2018)

Diego Bejarano (2017–2018)

Euirim Choi (2017–2018)

Ruth Francis Ng (2014–2015)

Professional service

Program committees and panels

Usenix Security '21, Usenix Security '20, WWW '17, ACSAC '16, ACSAC '15, ACSAC '14, NSF SaTC '14, EVT/WOTE '10

External reviews

DISC ’14, Usenix Security ’14, OSDI ’10, WWW ’10, CCS ’09, WWW ’09, Usenix ATC ’09, CCS ’08, WPES ’08

Journal reviews

Trans. on Cloud Computing Nov. ’16, Internet Computing May/Jun. ’16, Data Engineering Bulletin Dec. ’12, Trans. on Information and System Security Mar. ’10