Ariel J. Feldman

Assistant Professor
Department of Computer Science
University of Chicago

1100 East 58th Street
Chicago, IL 60637
arielfeldman@cs.uchicago.edu
https://arifeldman.com

Research interests

My research lies at the intersection of computer security and distributed systems. Topics that interest me include software and network security, data privacy, anonymity, and electronic voting. Much of my current work focuses on finding new ways to protect the security and privacy of users of "cloud hosted" services. I am also particularly interested in the interaction between computer security, law, and public policy.

Positions

7/14–present	**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, Inc.** (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*
Doctoral 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 Award, USENIX Security Symposium, 2008 and 2012

Princeton University Upton Fellowship, 2005

Brown University Ducasse Philosophy Award, 2002

Member of Phi Beta Kappa, 2002; Sigma Xi, 2003

Research

2012–present **Verifying stateful outsourced computation.** Enabling a client to outsource a program to a service provider and, in return, receive not only the result, but also a proof that the program executed correctly. Pantry [2], developed with Braun et al., is general purpose, supporting outsourcing of arbitrary programs written in a subset of C. Its security guarantees

depend solely on the hardness of cryptographic primitives, and not on assumptions about the provider's hardware or software. Unlike prior systems, it allows outsourced programs to compute over remote data that the client does not have, making it possible to verifiably run common cloud applications such as MapReduce jobs and database queries.

Proofs of correctness can also be zero-knowledge, enabling clients to verify computations on data that they not only do not possess, but are not allowed to see. VerDP [1] leverages this property to address a common problem in the publication of research studies: protecting the privacy of study participants makes it impossible for the results of the study to be repeatable. VerDP overcomes this conflict by enabling researchers to publish their results along with a publicly-verifiable proof that the researchers performed the claimed data analysis on the claimed data set without revealing the input data itself. Researchers write data analysis queries in a domain-specific language called VFuzz that is converted into a highly-parallelizable verifiable computation. VFuzz's type system also ensures that the published results are differentially-private, guaranteeing that they do not compromise the privacy of any individual study participant.

2009–present **Privacy and integrity in the untrusted cloud.** Allowing users to reap the benefits of cloud deployment while protecting the confidentiality and integrity of users' data even in the face of malicious cloud providers. SPORC [4] and Frientegrity [3] enable a wide variety of services which have security guarantees rooted in users' cryptographic keys rather than in providers' good intentions. In both systems, servers only observe encrypted data and cannot deviate from correct execution without detection. They also support dynamic access control even in the presence of concurrency.

SPORC supports collaborative applications such as word processing, calendaring, and email with an untrusted provider as well as concurrent, low-latency editing of shared state and disconnected operation. It not only allows users to detect a cloud provider's misbehavior, it allows them to recover from it, by switching providers and automatically repairing the inconsistencies that malicious servers may have caused. Frientegrity extends these guarantees to the scalability demands of online social networking services. In its novel method of detecting server equivocation, users collaborate so that none has to inspect every update, allowing users' feeds to scale to tens of thousands of updates. In addition, Frientegrity's access control and key distribution mechanisms scale efficiently to thousands of friends and tens of thousands of friends-of-friends.

2006–present **Electronic voting security.** Analyzed the security of two of the most widely-used electronic voting machines in the US and found serious vulnerabilities that enable an attacker to change votes, potentially without detection [8] [12]. Demonstrated a virus that would likely be able to spread automatically to a large population of voting machines, and showed that even a machine with significant hardware protections can be compromised via *return-oriented programming* [6]. Participated in California's "Top-to-Bottom" review of its voting equipment, which led the state to de-certify its insecure voting systems [13].

Demonstrated that, although cryptographic voting systems potentially make elections more verifiable and transparent, they suffer from ballot secrecy vulnerabilities that are more severe than previously believed. Presented a protocol that substantially mitigates this threat by preventing a compromised voting machine from maliciously manipulating the random values used in the encryptions of the votes [5].

2007–2008 **Cold boot attacks.** With Halderman et al., showed that DRAM retains its contents even after power is lost and even if it is removed from the motherboard. This phenomenon allows an attacker or forensic analyst to bypass the operating system's protections and obtain a full-system memory image including any cryptographic keys that it contains. Defeated several of the most popular disk encryption systems using this technique [7].

Refereed publications

[1] Arjun Narayan, **Ariel J. Feldman**, Antonis Papadimitriou, and Andreas Haeberlen. Verifiable

Differential Privacy. In *Proc. 2015 European Conference on Computer Systems (EuroSys '15)*, Bordeaux, France, April 2015.

[2] 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)*, Farmington, PA, November 2013.

[3] **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**.

[4] **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)*, Vancouver, BC, October 2010.

[5] **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)*, Montreal, QC, August 2009.

[6] 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)*, Montreal, QC, August 2009.

[7] 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)*, San Jose, CA, July 2008. **Awarded Best Student Paper**.

[8] **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)*, Boston, MA, August 2007.

Invited publications, technical reports, and other publications

[9] **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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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

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

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*

Professional service

Program committees and panels

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

References

Available on request.