Ben Adida

Curriculum Vitae

100 N Whisman Rd #4311
Mountain View, CA 94043
☎ *415.683.1383*
✉ *ben@adida.net*

Education

2003-2006 **PhD Computer Science**, *MIT*, Cambridge, MA.

1998-1999 **MEng Computer Science**, *MIT*, Cambridge, MA.

1994-1998 **S.B. Computer Science**, *MIT*, Cambridge, MA.

PhD thesis

title Advances in Cryptographic Voting Systems

supervisors Ronald L. Rivest, Shafi Goldwasser, Srinivas Devadas

Academic Research

2007-present **Instructor and Research Faculty**, *Harvard Medical School*, Boston, MA.
medical informatics research, with a focus on personally-controlled health record, health-data software platforms, and health-data security.

2006-2008 **Postdoctoral Fellow**, *Harvard University*, Cambridge, MA.
privacy and security research, with a focus on voting systems.

2004-2006 **Research Assistant**, *MIT*, Cambridge, MA.
voting systems.

1998-1999 **Research Assistant**, *MIT*, Cambridge, MA.
voting systems and general security.

Industry Experience

2002 - present **Technical Advisor and W3C Representative**, *Creative Commons*, San Francisco, CA.
Machine-readable markup, specifically semantic web, and more generally web technology.

2005 **Consultant**, *Children's Hospital Boston*, Boston, MA.
Performed security review of source code for Personally Controlled Health Record (PCHR) system. Designed and developed a new secure and efficient storage mechanism for genomic data.

2000-2003 **Co-Founder, CEO and CTO**, *OpenForce*, New York, NY.
Defined and implemented company business plan: providing enterprise web software services using open-source software. Often hired as acting Chief Technology Officer by customers (GreenOrder, Creative Commons). Signed on, architected, and led the software implementation of client projects, including the MIT Sloan School of Management, the LA Unified School District, GreenPeace, Creative Commons, GreenOrder, the Berklee School of Music.

1999-2002 **Co-Founder and Director**, *OpenACS and dotLRN open-source projects*.
Led design and implementation of major open-source enterprise web software endeavors: the OpenACS web application toolkit and dotLRN course management system. More than 15 companies support this software and hundreds of web sites run it, including more than 100 universities.

1998-1999 **Co-Founder and Project Lead**, *ArsDigita*.
Led design, implementation, and deployment of major software projects with Levi Strauss and GreenTravel.com (now Away.com). Helped launch the first open-source web application toolkit in 1998: the ArsDigita Community System.

Publications

Ben Adida. *Advances in Cryptographic Voting Systems*. PhD thesis, August 2006. PhD Thesis, MIT.

Ben Adida. BeamAuth: Two-Factor Web Authentication with a Bookmark. In *CCS 2007, Proceedings of the Fourteenth ACM Conference on Computer and Communications Security*, October 2007.

Ben Adida. The Browser as a Secure Platform for Loosely Coupled Private-Data Mashups. In *W2SP 2007, Proceedings of the First Workshop on Web 2.0 Security & Privacy, Oakland, CA, USA*, May 2007.

Ben Adida. The Mobile Browser as a Web-Based Platform for Identity, Sep 2007.

Ben Adida. EmID: Web Authentication by Email Address. In *W2SP 2008, Proceedings of the Second Workshop on Web 2.0 Security & Privacy, Oakland, California.*, May 2008.

Ben Adida. Helios: Web-based Open-Audit Voting. In *Proceedings of the Seventeenth Usenix Security Symposium (USENIX Security 2008)*, pages 335–348, July 2008.

Ben Adida. hGRDDL: Bridging microformats and RDFa. *J. Web Sem.*, 6(1):54–60, 2008.

Ben Adida. SessionLock: Securing Web Sessions against Eavesdropping. In *WWW 2008, Proceedings of the Seventeenth World Wide Web Conference, Beijing China.*, April 2008.

Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Ross Anderson, and Ronald L. Rivest. On the Security of the EMV Secure Messaging API. In *SPW 2007, Proceedings of the Fifteenth International Workshop on Security Protocols, Brno, Czech Republic*, April 2007.

Ben Adida, David Chau, Susan Hohenberger, and Ronald L. Rivest. Lightweight Email Signatures. In Jakobsson and Myers, editors, *Phishing and Countermeasures*. Wiley, 2006.

Ben Adida, David Chau, Susan Hohenberger, and Ronald L. Rivest. Lightweight Email Signatures (Extended Abstract). In *Fifth Conference on Security and Cryptography for Networks (SCN'06)*, volume 4116 of *Lecture Notes in Computer Science*, pages 288–302. Springer Verlag, 2006.

Ben Adida, Olivier deMarneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios. In *EVT/WOTE 2009, Proceedings of the Electronic Voting Technology Workshop / Workshop on Trustworthey Elections, August 10th 2009, Montreal,Canada.*, 2009.

Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Lightweight Encryption for Email. In *Proceedings of USENIX's First Steps to Reducing Unwanted Traffic on the Internet (SRUTI) 2005*, pages 93–99, July 2005.

Ben Adida and Isaac Kohane. GenePING: secure, scalable management of personal genomic data. *BMC Genomics*, 7(1):93, 2006.

Ben Adida and C. Andrew Neff. Ballot Casting Assurance. In *EVT '06, Proceedings of the First Usenix/ACCURATE Electronic Voting Technology Workshop, August 1st 2006, Vancouver, BC,Canada.*, 2006.

Ben Adida and C. Andrew Neff. Efficient Receipt-Free Ballot Casting Resistant to Covert Channels. In *EVT/WOTE 2009, Proceedings of the Electronic Voting Technology Workshop / Workshop on Trustworthey Elections, August 10th 2009, Montreal,Canada.*, 2009.

Ben Adida and Ronald L. Rivest. Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting. In Roger Dingledine and Ting Yu, editors, *ACM Workshop on Privacy in the Electronic Society*. ACM, October 2006.

Ben Adida and Douglas Wikström. How to Shuffle in Public. In *Theory of Cryptography, Proceedings of TCC 2007*, Lecture Notes in Computer Science, pages 555–574. Springer-Verlag, February 2007.

Ben Adida and Douglas Wikström. Offline/Online Mixing. In Christian Cachin, editor, *ICALP 2007, Proceedings of the Thirty-Fourth International Colloquium on Automatata, Languages, and Programming, Wroclaw, Poland*, July 2007.

Mark Levine, Ben Adida, Kenneth Mandl, Isaac Kohane, and John Halamka. What are the benefits and risks of fitting patients with radiofrequency identification devices? *PLoS Med*, 4(11):e322, 11 2007.

Poorvi L. Vora, Ben Adida, R. Bucholz, D. Chaum, D. L. Dill, David Jefferson, D. W. Jones, W. Lattin, Aviel D. Rubin, M. I. Shamos, and Moti Yung. Evaluation of voting systems. *Commun. ACM*, 47(11):144, 2004.

Paul Youn, Ben Adida, Mike Bond, Jolyon Clulow, Jonathan Herzog, Amerson Lin, Ross Anderson, and Ronald L. Rivest. Robbing the Bank with a Theorem Prover. In *SPW 2007, Proceedings of the Fifteenth International Workshop on Security Protocols, Brno, Czech Republic*, April 2007.

Invited Presentations

available for download at `http://ben.adida.net/presentations/`.

Cryptography and Voting

August 2009 **EVT/WOTE 2009**, *Invited Talk*.

Helios – Real-World Open-Audit Voting

May 2009 **Electronic Voting Workshop, Tel Aviv University**, *Invited Talk*.

Voting Security – an Overview

May 2008 **Electronic Voting Workshop, IDC**, *Invited Talk*.

Open-Audit Voting: How to let anyone verify an election

February 2009 **Universite catholique de Louvain**, *Guest Lecture*.

Secure Voting

October 2008 **Harvard College Fund Assembly**, *Invited Talk*.

Verifying Elections with Cryptography

December 2007 **Google**, *Invited Talk*.

Web (2.0) Security

April 2007 **Harvard University**, *CRCS Seminar*.

Beyond the Paper Trail

February 2007 **IEEE Society on Societal Implications of Technology**, *Invited Talk*.

Public Mixing for Open-Audit Elections

December 2006 **Harvard University**, *Theory Seminar*.

November 2006 **Stanford University**, *Invited Talk*.

November 2006 **UC Berkeley**, *Invited Talk*.

Open-Audit Elections

November 2006 **Google**, *Invited eng.Edu Seminar*.

November 2006 **SRI**, *Invited Talk*.

Transparent Elections

November 2006 **Wellesley College**, *Invited Talk*.

A Brief History of Secure Voting

September 2006 **Harvard University**, *CRCS Seminar*.

Privacy in an Always-Online World

July 2006 **MIT Media Laboratory**, *Simplicity 2006*.

Introduction to Cryptography

May 2006 **MIT Course – Quantitative Foundations of Engineering Systems**, *Guest Lecture*.

Web Security

May 2006 **MIT Course – Software Engineering for Internet Applications**, *Guest Lecture*.

November 2003 **MIT Course – Software Engineering for Internet Applications**, *Guest Lecture*.

Direct Verification of Elections with Cryptography

April 2006 **University of Massachusetts at Amherst**, *Guest Lecture*.

Lightweight Signatures for Email

December 2005 **MIT Course – Network and Computer Security**, *Guest Lecture*.

December 2005 **MIT/Cisco Security Summit**, *Invited Talk*.

November 2005 **Harvard University**, *CRCS Seminar*.

August 2005 **Google**, *Invited Talk*.

May 2005 **MIT**, *Cryptography and Information Security Seminar*.

Cryptographic Voting

February 2005 **Radcliffe Institute for Advanced Study**, *Invited Talk*.

Robusts Mixnets in Electronic Voting

January 2005 **Cambridge University**, *Invited Talk*.

Trusting the Vote

December 2004 **Harvard Law School – Internet and Society Conference**, *Invited Talk*.

Secure and Fair Elections

November 2004 **Harvard Law School and MIT Course – Digital Democracy**, *Guest Lecture*.

Teaching and Advising

2006 - present **Advisor to PhD students, Medical Informatics Fellows**, *Harvard Medical School*.
Reader for Collin Jackson, PhD Stanford 2009. Advisor to pre-doctoral and post-doctoral fellows at Harvard Medical School.

2004 - 2006 **Advisor to Undergraduates and Masters' Students**, *MIT*.
Provided guidance to Undergraduate and Masters' students in security and cryptography: David Chau, Dan Williams, Amerson Lin, Joy Forsythe.

Fall 2003 **Software Engineering for Internet Applications (6.171)**, *MIT*, Teaching Assistant.
Helped design the course and problem sets, coordinated 10 student software development teams, graded all problem sets and midterm. Rated 6.5/7.0 by student-led course guide.

Fall 1999 **Software Engineering for Web Applications (6.916)**, *MIT*, Teaching Assistant.
Helped design the first version of this course, which became a mainstream MIT course a couple years later. Developed and maintained the software platform for students to use.

Spring 1998 **Structure and Interpretation of Computer Programs (6.001)**, *MIT*, Teaching Assistant.
Taught 8 weekly hours of tutorials. Graded problem sets, quizzes, and exams.

Fall 1996 **Introduction to Interactive Programming (6.096)**, *MIT*, Lab/Teaching Assistant.
Helped design the first version of this course. Developed software for problem sets.

Conferences, Journals, and Standards Committees

Program Committees and Reviews

2010 **USENIX HealthSec**, *Program Committee*.

2008,2009,2010 **WWW Conference, Security and Privacy Track (WWW)**, *Program Committee*.

2008,2009,2010 **Web 2.0 Security and Privacy (W2SP)**, *Program Committee*.

2008,2010 **ACM Computer and Communication Security (CCS)**, *Program Committee*.

2008,2010 **Applied Cryptography and Network Security (ACNS)**, *Program Committee*.

2009 **IEEE Security and Privacy (Oakland)**, *Program Committee*.

2009 **International Semantic Web Conference (ISWC) Workshop on Semantics for the Rest of Us**, *Program Committee*.

2009 **Electronic Voting Technology Workshop/ Workshop on Trustworthy Elections (EVT/WOTE)**, *Program Committee*.

2007,2008 **USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)**, *Program Committee*.

2008 **Workshop on Trustworthy Elections (WOTE)**, *Program Committee Co-Chair*.

2007 **ACM Workshop on Privacy in the Electronic Society**, *Program Committee*.

2006 **Workshop on Trustworthy Elections (WOTE)**, *Program Committee*.

2004 - present **Journal Reviewer**, *various crypto/security journals*.
ACM Computer Communications Review, ACM Transactions on Information Security, Discrete Applied Mathematics, IEEE Transactions on Computers, ACM Transactions on Internet Technology.

2004 - present **External Reviewer**, *various crypto/security conferences*.
PKC 2005, PKC 2006, IEEE Security and Privacy 2006, Eurocrypt 2007, ACNS 2007, STACS 2007.

Standards Committees and Working Groups

2009-present **W3C**, *HTML Working Group*, Member.

2006-present **W3C**, *Semantic Web Deployment Working Group*, RDF-in-HTML Task Force Chair.

2006-present **StopBadware**, *Working Group*, Berkman Center at Harvard University.

2002-2003 **Center for Strategic and International Studies (CSIS)**, *Authentication Working Group*.