

Ben Adida

469 Shawmut Ave #2 - Boston, MA 02118
ben@adida.net - <http://ben.adida.net>

PROFILE

Specialized in cryptography applied to public policy, including voting systems, authentication infrastructures, and secure health records. Extensive experience in all aspects of web software, including database design and semantic web. Extensive industry experience in software development and the management of software development teams.

EDUCATION

Massachusetts Institute of Technology 2003-2006

PhD in Computer Science, *August 2006*.

Thesis: Advances in Cryptographic Voting Systems

Advisor: Ronald L. Rivest

Massachusetts Institute of Technology 1998-1999

MEng in Computer Science, June 1999.

Thesis: Self-Describing Cryptography Through Certified Universal Code

Advisor: Ronald L. Rivest

Massachusetts Institute of Technology 1994-1998

SB in Computer Science, June 1998.

RESEARCH EXPERIENCE

Harvard Center for Research on Computation and Society - Postdoctoral Fellow 2006-present
Research on security and privacy in voting, health records, and web applications.

Cambridge-MIT Institute - Research Assistant 2004-2006
Research on the security of cryptographic APIs

Caltech/MIT Voting Technology Project - Research Assistant 2004-2006
Research on universally-verifiable voting.

MIT Lab for Computer Science - Research Assistant 1998-1999
Research on voting systems and self-describing cryptography.

INDUSTRY EXPERIENCE

Children's Hospital Informatics Program (Boston) - Consultant *May - Aug 2005*
Performed security review of source code for Personal Health Record management system, designed and implemented fixes at cryptographic and application security levels. Designed and developed a new secure and efficient storage mechanism for genomic data.

OpenForce - co-founder, CEO & CTO 2000-2003
Defined and implemented the company business plan: providing enterprise internet software services. Often hired as acting Chief Technology Officer by customers (GreenOrder, Creative Commons). Responsible for signing on, architecting, and leading 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.

OpenACS & dotLRN open-source projects - co-founder and director 1999-2002
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.

ArsDigita - founding member 1998-1999
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.

RSA Data Security - developer summer 1997
Co-developed the first Java cryptography toolkit (JSAFE 1.0).

Sun Labs - developer summer 1996
Implemented `java.lang.Math` in pure Java for Java-only platforms.
Instrumented the Java Virtual Machine for collecting statistics about garbage collection.

REFEREED PUBLICATIONS

“HOW TO SHUFFLE IN PUBLIC,” with Douglas Wikström, to appear in *Proceedings of the Fourth Theory of Cryptography Conference (TCC 2007)*, February 2007. Preliminary version on eprint: <http://eprint.iacr.org/2005/394>

“SCRATCH & VOTE: SELF-CONTAINED PAPER-BASED CRYPTOGRAPHIC VOTING,” with Ronald L. Rivest in *Proceedings of the Workshop on Privacy in the Electronic Society (WPEs) 2006*, October 2006.

“LIGHTWEIGHT EMAIL SIGNATURES,” with David Chau, Susan Hohenberger, and Ronald L. Rivest in *Proceedings of the Fifth Conference on Security and Cryptography in Networks (SCN) 2006*, September 2006.

“BALLOT CASTING ASSURANCE,” with C. Andrew Neff in *Proceedings of the First USENIX/ACCURATE Electronic Voting Technology Workshop (EVT) 2006*, August 2006.

“GENEPING: SECURE, SCALABLE MANAGEMENT OF PERSONAL GENOMIC DATA”, with Isaac S. Kohane, in *BioMed Central Genomics 2006 7:93*, April 2006.

“LIGHTWEIGHT ENCRYPTION FOR EMAIL,” with Susan Hohenberger and Ronald L. Rivest in *Proceedings of USENIX's First Steps to Reducing Unwanted Traffic on the Internet (SRUTI) 2005*, pages 93-99, July 2005.

“EVALUATION OF VOTING SYSTEMS,” with P. Vora, R. Bucholz, D. Chaum, D.L. Dill, D. Jefferson, D.W. Jones, W. Lattin, A.D. Rubin, M. I. Shamos, M. Yung in *Communications of the ACM*, page 144, November 2004.

FORTHCOMING PUBLICATIONS

“AD-HOC GROUP SIGNATURES FROM HIJACKED KEYPAIRS,” with Susan Hohenberger and Ronald L. Rivest, preliminary version in *Proceedings of DIMACS Workshop on Theft in Electronic Commerce*, April 2005.

“A FAST APPROXIMATION OF REENCRYPTION MIXNET PROOFS,” with Ronald L. Rivest, *in preparation*.

“ON THE SECURITY OF THE EMV SECURITY API,” with Mike Bond, Jolyon Clulow, Amerson Lin, Ross Anderson and Ronald L. Rivest, *in submission*.

“(ALMOST) ROBBING THE BANK WITH A THEOREM PROVER,” with Paul Youn, Mike Bond, Jolyon Clulow, Jonathan Herzog, Amerson Lin, Ross Anderson and Ronald L. Rivest, *in submission*.

“BUILDING INTEROPERABLE METADATA,” with Hal Abelson, *in preparation*.

INVITED PRESENTATIONS

PUBLIC MIXING FOR OPEN-AUDIT ELECTIONS

Lecture at Stanford
Lecture at UC Berkeley

November 2006
November 2006

OPEN-AUDIT ELECTIONS

Lecture at Google eng.Edu
Lecture at SRI International

November 2006
November 2006

TRANSPARENT ELECTIONS

Lecture at Wellesley College

November 2006

SCRATCH & VOTE: SELF-CONTAINED PAPER-BASED CRYPTOGRAPHIC VOTING

Presentation at Workshop on Privacy in the Electronic Society 2006.

October 2006

SECURE VOTING PROTOCOLS

MIT Distributed Systems Group Seminar

September 2006

A BRIEF HISTORY OF SECURE VOTING

Harvard CRCS Seminar

September 2006

PRIVACY IN AN ALWAYS-ONLINE WORLD

Simplicity 2006, MIT Media Laboratory

July 2006

INTRODUCTION TO CRYPTOGRAPHY

Lecture in MIT's 6.976 - Quantitative Foundations of Engineering Systems

May 2006

WEB SECURITY

Lecture in MIT's 6.171 - Software Engineering for Internet Applications

May 2006

DIRECT VERIFICATION OF ELECTIONS WITH CRYPTOGRAPHY

Lecture at ARIA, University of Massachusetts at Amherst

April 2006

LIGHTWEIGHT SIGNATURES FOR EMAIL

Lecture in MIT's Network and Computer Security Class (6.857)

December 2005

MIT/Cisco Security Summit

December 2005

Harvard's Center for Research in Computation and Society

November 2005

Google, Palo Alto

August 2005

MIT's Decentralized Information Group

May 2005

MIT's Cryptography and Information Security Seminar

May 2005

LIGHTWEIGHT ENCRYPTION FOR EMAIL

Steps to Reducing Unwanted Traffic on the Internet, Cambridge, MA.

July 2005

CRYPTOGRAPHIC VOTING TUTORIAL

Radcliffe Institute for Advanced Study, Harvard University, Cambridge, MA.

February 2005

ROBUST MIXNETS IN ELECTRONIC VOTING

Cambridge University, Cambridge, England.

January 2005

TRUSTING THE VOTE

Internet & Society Conference, Harvard Law School

December 2004

SECURE AND FAIR ELECTIONS

Digital Democracy, joint class of the Harvard Law School and MIT

November 2004

WEB SECURITY

Lecture in MIT's Software Engineering for Internet Applications (6.171)

November 2003

TEACHING AND ADVISING EXPERIENCE

Advisor to Undergraduates and Master's Students

2004-present

Provided guidance to Undergraduate and Master's students in security and cryptography:
David Chau, Dan Williams. Amerson Lin, Joy Forsythe.

Software Engineering for Internet Applications (6.171) - Teaching Assistant

Fall 2003

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.

Structure and Interpretation of Computer Programs (6.001) - Teaching Assistant

Spring 1998

Taught 8 weekly hours of tutorials. Graded problem sets, quizzes, and exams.

Software Engineering for Web Applications (6.916) - Teaching Assistant

Fall 1999

Helped design the first version of this course. Developed and maintained the software platform for students to use.

Introduction to Interactive Programming (6.096) - Lab/Teaching Assistant

Fall 1996

Helped design the first version of this course. Developed software for problem sets.

PROFESSIONAL ACTIVITIES

USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)

Member of Program Committee.

August 2007

Workshop On Trustworthy Elections (WOTE)

Member of Program Committee.

July 2006

External Conference and Journal Reviewer

2004-present

PKC 2005, ACM CCR Journal, PKC 2006, IEEE Security & Privacy 2006, Eurocrypt 2007, ACNS 2007.

Harvard Law School, Berkman Center StopBadware - Working Group Member

2006-present

Advisor on spyware research working group in association with Google, Sun, and Lenovo.

Harvard Medical School, Countway Library - Member, Technology Advisory Board

2005-present

Advisor on web development and semantic web issues.

W3C - Chair, RDF-in-XHTML Task Force, Semantic Web Best Practices Working Group

2004-present

Leading a team of industry experts drawn from the W3C's Semantic Web and HTML working groups to specify mechanisms for including semantic web statements (RDF) in HTML. Developing the RDFa standard. Primary author of the RDFa syntax and primer documents.

Harvard Law School Berkman Center - Associate

2003-present

Advisor to the Berkman Center on technology issues.

Creative Commons - Member, Technology Advisory Board

2003-present

Advisor on web development issues, particular focus on semantic web. Representative to the W3C.

Center for Strategic & International Studies - Member, Authentication Working Group
Developed recommendations on Federated Authentication systems.

2002-2003

REFERENCES

Ronald L. Rivest

Professor of Computer Science, MIT
The Stata Center at MIT
32 Vassar Street, Room G692
Cambridge, MA 02139
rivest@mit.edu

Hal Abelson

Professor of Computer Science, MIT
The Stata Center at MIT
32 Vassar Street, Room 386
Cambridge, MA 02139
hal@mit.edu

Lawrence Lessig

Professor of Law, Stanford
Stanford Law School, Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
lessig@pobox.com

Daniel J. Weitzner

Technology and Society Domain Leader, W3C
The Stata Center at MIT
32 Vassar Street, Room G516
Cambridge, MA 02139
djweitzner@w3.org