

# Ari Juels

RSA Laboratories  
11 Cambridge Center  
Cambridge, MA 02142  
Telephone: 617.300.7155  
E-mail: [ajuels@rsa.com](mailto:ajuels@rsa.com)  
Web: [www.ari-juels.com](http://www.ari-juels.com)

## PROFESSIONAL ROLE

As Chief Scientist and Director of RSA Laboratories, I oversee its research program and staff. RSA Laboratories' charter is to produce research with practical impact on the products and strategy of RSA and its parent company EMC and scholarly influence in the larger research community. My personal areas of research interest include user authentication, biometrics, financial cryptography, RFID, network security, storage security, and electronic voting.

## INDUSTRY EXPERIENCE

<b>Chief Scientist and Director</b>	RSA Laboratories	2007 -
<b>Principal Research Scientist</b>	RSA Laboratories	1999 - 2007
<b>Senior Research Scientist</b>	RSA Laboratories	1998 - 1999
<b>Research Scientist</b>	RSA Laboratories	1996 - 1998
<b>Co-founder</b>	RavenWhite Inc.	2006 -

## EDUCATION

<b>Ph.D.</b>	University of California at Berkeley Computer Science Division Dissertation: <i>Topics in Black-Box Combinatorial Optimization</i> Advisor: Prof. Alistair Sinclair	1991-96
<b>B.A.</b>	Amherst College, Amherst, MA Mathematics and Latin Literature Phi Beta Kappa	1987-91

## RESEARCH PAPERS

- A. Oprea and A. Juels. A Clean-Slate Look at Disk Scrubbing. In submission, 2009.
- M. Jakobsson and A. Juels. Server-Side Detection of Malware Infection. New Security Paradigms Workshop, 2009.
- K. Koscher, A. Juels, T. Kohno, and V. Brajkovic. EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. ACM CCS, 2009. To appear.
- K. Bowers, A. Juels, and A. Oprea. HAIL: A High-Availability and Integrity Layer for Cloud Storage. ACM CCS, 2009. To appear. Draft available at [eprint.iacr.org/2008/489](http://eprint.iacr.org/2008/489).
- M. Salajegheh, S. Clark, B. Ransford, K. Fu, and A. Juels. CCCP: Secure Remote Storage for Computational RFIDs. USENIX Security, 2009.

- K. Bowers, A. Juels, and A. Oprea. Proofs of Retrievability: Theory and Implementation. In submission, 2009. Draft available at <http://eprint.iacr.org/2008/175>.
- T. Kohno. An Interview with RFID Security Expert Ari Juels. *IEEE Pervasive Computing*, 7(1):10-11, 2008.
- A. Juels, B. Parno, and R. Pappu. Unidirectional Key Distribution Across Time and Space with Applications to RFID Security. *USENIX Security*, 2008.
- M. Jakobsson, A. Juels, and Jacob Ratkiewicz. Privacy-Preserving History Mining for Web Browsers. *W2SP*, 2008.
- S.G. Choi, A. Elbaz, A. Juels, T. Malkin, and M. Yung. Two-Party Computing with Encrypted Data. *Asiacrypt '07*. 2007.
- D. Bailey, D. Boneh, E.-J. Goh, and A. Juels. Covert Channels in Privacy-Preserving Identification Systems. In S. De Capitani di Vimercati and P. Syverson, eds., *14th ACM Conference on Computer and Communications Security (ACM CCS)*, 2007.
- A. Juels and B. Kaliski. PORs: Proofs of Retrievability for Large Files. In S. De Capitani di Vimercati and P. Syverson, eds., *14th ACM Conference on Computer and Communications Security (ACM CCS)*, 2007.
- T. Heydt-Benjamin, D. Bailey, K. Fu, A. Juels, and T. O'Hare. Vulnerabilities in First-Generation RFID-Enabled Credit Cards. In S. Dietrich, ed., *Financial Cryptography and Data Security*, 2007.
- B. Defend, K. Fu, and A. Juels. Cryptanalysis of Two Lightweight RFID Authentication Schemes. In *PerSec*, 2007.
- A. Juels and S. Weis. Defining Strong Privacy for RFID. In *PerTec*, 2007. Full paper to appear in *ACM TISSEC* in 2009.
- A. Juels, S. Stamm, and M. Jakobsson. Combating Click Fraud via Premium Clicks. In A. Keromytis, ed., *USENIX Security*, 2007.
- J. Brainard, A. Juels, R. Rivest, M. Szydlo, and M. Yung. Fourth-Factor Authentication: Someone You Know. In A. Juels, R. N. Wright, and S. De Capitani di Vimercati, eds., *13th ACM Conference on Computer and Communications Security (ACM CCS '06)*, pp. 168–78, 2006.
- D. Bailey and A. Juels. Shoehorning Security into the EPC Standards. In R. De Prisco and M. Yung, eds., *Security and Cryptography for Networks (SCN '06)*, pp. 303–320, 2006.
- J. Halamka, A. Juels, A. Stubblefield, and J. Westhues. The Security Implications of VeriChip Cloning. In *Journal of the American Medical Informatics Association (JAMIA)*, 13(6):601–607, November 2006.
- A. Juels, M. Jakobsson, and T. Jagatic. Cache Cookies for Browser Authentication (Extended Abstract). In V. Paxson and B. Pfizmann, eds., *IEEE Symposium on Security and Privacy*, pp. 301–305, 2006.
- A. Juels. RFID Security and Privacy: A Research Survey. *Journal of Selected Areas in Communication (J-SAC)*, 24(2):381–395, February 2006. Recipient of 2007 IEEE Best Tutorial Paper Award.
- A. Juels, D. Molnar, and D. Wagner. Security and Privacy Issues in E-passports. In D. Gollman, L. Gong, and G. Tsudik, eds., *SecureComm '05*. IEEE Press, 2005.
- A. Juels and S. Weis. Authenticating Pervasive Devices with Human Protocols. In V. Shoup, ed., *Advances in Cryptology – Crypto '05*, pp. 293–308. Springer-Verlag, 2005.

- A. Juels, D. Catalano, and M. Jakobsson. Coercion-Resistant Electronic Elections. In R. Dingledine and S. De Capitani di Vimercati, eds., *Workshop on Privacy in the Electronic Society*, pp. 61–70. ACM Press, 2005.
- A. Juels. Strengthening EPC Tags Against Cloning. In M. Jakobsson and R. Poovendran, eds., *ACM Workshop on Wireless Security*, pp. 67–75. ACM Press, 2005.
- A. Juels, P. Syverson, and D. Bailey. High-Power Proxies for Enhancing RFID Privacy and Utility. In G. Danezis and D. Martin, eds., *Workshop on Privacy Enhancing Technologies*, pp. 210–226. Springer-Verlag, 2005.
- S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security Analysis of the a Cryptographically Enabled RFID Device. In P. McDaniel, ed., *USENIX Security*, pp. 1-14. 2005. Recipient of Best Student Paper Award, USENIX Security and Outstanding Research Award in Privacy Enhancing Technologies for the year 2007.
- S. Garfinkel, A. Juels, and R. Pappu. RFID Privacy: An Overview of Problems and Proposed Solutions. In *IEEE Security and Privacy*, 3(3): 34-43. May/June 2005.
- A. Juels. Minimalist Cryptography for RFID Tags. In C. Blundo and S. Cimato, eds., *Fourth Conference on Security of Communication Networks*, pp. 149–164. Springer-Verlag, 2004.
- A. Juels and J. Brainard. Soft Blocking: Flexible Blocker Tags on the Cheap. In S. De Capitani di Vimercati and P. Syverson, eds., *Workshop on Privacy in the Electronic Society*, pp. 1–7. ACM Press, 2004.
- B. Waters, A. Juels, A. Halderman, and E. Felten. New Client Puzzle Outsourcing Techniques for DoS Resistance. In B. Pfitzmann and P. McDaniel, eds., *11th ACM Conference on Computer and Communications Security*, pp. 246–256. ACM Press, 2004.
- P. Golle and A. Juels. Parallel Mixing. In B. Pfitzmann and P. McDaniel, eds., *11th ACM Conference on Computer and Communications Security*, pp. 220 – 226. ACM Press, 2004.
- P. Golle and A. Juels. Dining Cryptographers Revisited. In C. Cachin and J. Camenisch, eds., *Advances in Cryptology – Eurocrypt ’04*. Springer-Verlag, 2004, pp. 456–473.
- A. Juels. “Yoking-Proofs” for RFID Tags. In R. Sandhu and R. Thomas, eds., *First International Workshop on Pervasive Computing and Communication Security*, pp. 138–143. IEEE Press, 2004.
- P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal Re-Encryption for Mixnets. In T. Okamoto, ed., *RSA Conference Cryptographers’ Track ’04*, pages 163–178. Springer-Verlag, 2004.
- A. Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In V. Atluri, ed., *10th ACM Conference on Computer and Communications Security*, pp. 103–111. ACM Press, 2003.
- J. Brainard, A. Juels, B. Kaliski, and M. Szydlo. A New Two-Server Approach for Authentication with Short Secrets. In V. Paxson, ed., *USENIX Security ’03*, pp 201–214. 2003. (A paper about the Nightingale system.)
- A. Juels and R. Pappu. Squealing Euros: Privacy-Protection in RFID-Enabled Banknotes. In R. Wright, ed., *Financial Cryptography ’03*, pages 103–121. Springer-Verlag, 2003.
- P. Golle, S. Zhong, D. Boneh, M. Jakobsson, and A. Juels. Optimistic Mixing for Exit Polls. *Advances in Cryptology – ASIACRYPT ’02*, pages 451–465. Springer-Verlag, 2002.
- A. Juels and J. Guajardo. RSA Key Generation with Verifiable Randomness. In D. Naccache and P. Paillier, eds., *Public Key Cryptography 2002*, pages 357–374. Springer-Verlag, 2002.

- A. Juels and M. Sudan. A Fuzzy Vault Scheme. *Designs, Codes, and Cryptography*, 38(2): 237 – 257, February 2006. One-page abstract appeared in A. Lapidot and E. Teletar, eds., Proceedings of IEEE International Symposium on Information Theory, p.408, IEEE Press, Lausanne, Switzerland, 2002.
- M. Jakobsson, A. Juels, and R. L. Rivest. Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking. In D. Boneh, ed., *USENIX Security '02*, pp. 339–353. 2002.
- A. Juels and M. Szydło. A Two-Server Auction Protocol. In M. Blaze, ed., *Financial Cryptography '02*, pages 72–86. Springer-Verlag, 2002.
- M. Jakobsson, A. Juels, and P. Q. Nguyen. Proprietary Certificates. In B. Preneel, ed., *RSA Security Conference 2002 Cryptographers' Track*, pages 164–181. Springer-Verlag, 2001.
- M. Jakobsson and A. Juels. An Optimally Robust Hybrid Mix Network. In *Principles of Distributed Computing (PODC) '01*, pages 284–292. ACM Press, 2001.
- N. Frykholm and A. Juels. Error-Tolerant Password Recovery. In P. Samarati, ed., *8th ACM Conference on Computer and Communications Security*, pages 1–8. ACM Press, 2001.
- A. Juels. Targeted Advertising... and Privacy Too. In D. Naccache, ed., *RSA Security Conference 2001 Cryptographers' Track*, pages 408–424. Springer-Verlag, 2001.
- M. Jakobsson and A. Juels. Mix and Match: Secure Function Evaluation via Ciphertexts, In T. Okamoto, ed., *Advances in Cryptology – ASIACRYPT '00*, pages 346–358. Springer-Verlag, 2000.
- M. Jakobsson and A. Juels. Addition of El Gamal Plaintexts, In T. Okamoto, ed., *Advances in Cryptology – ASIACRYPT '00*, pages 346–358. Springer-Verlag, 2000.
- J. Håstad, J. Jonsson, A. Juels, and M. Yung. Funkspiel Schemes: An Alternative to Conventional Tamper Resistance. In S. Jajodia, ed., *7th ACM Conference on Computer and Communications Security*, pages 125–133. ACM Press, 2000.
- A. Juels and M. Wattenberg. A Fuzzy Commitment Scheme. In G. Tsudik, ed., *6th ACM Conference on Computer and Communications Security*, pages 28–36. ACM Press, 1999.
- A. Juels, M. Jakobsson, E. Shriver, and B. Hillyer. How to Turn Loaded Dice into Fair Coins. In *IEEE Transactions on Information Theory*, 46 (3): 911–921, May 2000.
- M. Jakobsson and A. Juels. Proofs of Work and Bread Pudding Protocols, In B. Preneel, ed., *Communications and Multimedia Security*, pages 258–272. Kluwer Academic Publishers, 1999.
- A. Juels and J. Brainard. Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks. In S. Kent, ed., *Networks and Distributed Security Systems '99*, pages 151–165. 1999.
- A. Juels. Trustee Tokens: Simple and Practical Tracing of Anonymous Digital Cash. In R. Hirschfeld, ed., *Financial Cryptography '99*, pages 29–45. Springer-Verlag, 1999.
- M. Jakobsson, L. Shriver, B. Hillyer, and A. Juels. A Practical Secure Physical Random Bit Generator. In M. Reiter, ed., *5th ACM Conference on Computer and Communications Security*, pages 103–111. ACM Press, 1998.
- A. Juels and M. Peinado. Hiding Cliques for Cryptographic Security. In *9th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, ACM Press, 1998. Journal version in *Designs, Codes, and Cryptography*, 20(3):269–280, July 2000.
- M. Jakobsson and A. Juels. X-cash: Executable Digital Cash. In R. Hirschfeld, ed., *Financial Cryptography '98*, pages 16–27. Springer-Verlag, 1998.
- A. Juels, M. Luby, and R. Ostrovsky. Security of Blind Digital Signatures. In B. S. Kaliski Jr., ed., *Advances in Cryptology – CRYPTO '97*, LNCS No. 1294, pages 150–164. Springer-Verlag, 1997.

A. Juels and M. Wattenberg. Hillclimbing as a Baseline Method for the Evaluation of Stochastic Optimization Algorithms. In D. S. Touretzky et al., eds., *Advances in Neural Information Processing Systems 8*, pages 430–436. MIT Press, 1995.

## BOOKS

A. Juels. *Tetraktys*. Emerald Bay Books, 2009. (A thriller novel.)

## BOOK CHAPTERS / EDITED VOLUMES / GUEST ARTICLES

A. Juels. The Vision of Secure RFID. *Proceedings of the IEEE*, 95(8):1–2, August 2007.

A. Juels, R. N. Wright, and S. De Capitani di Vimercati, eds., *13th ACM Conference on Computer and Communications Security*, ACM Press, 2006.

A. Juels. “The Limitations of Perfect User Authentication.” *Phishing and Anti-Phishing*, M. Jakobsson and S. Myers, eds., John Wiley & Sons, 2006.

A. Juels. “Cryptography.” *Handbook of Computer Networks*, H. Bigdoli, ed., John Wiley & Sons, 2006.

V. Atluri, C. Meadows, and A. Juels, eds., *12th ACM Conference on Computer and Communications Security*, ACM Press, 2005.

A. Juels. “A Bit of Privacy.” In *RFID Journal*, 2 May 2005. Guest column.

A. Juels. “Attack on a Cryptographic RFID Device.” In *RFID Journal*, 28 Feb. 2005. Guest column.

A. Juels. “RFID Privacy: A Technical Primer for the Non-Technical Reader.” *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. D.S. Raicu and K. Strandburg, eds., Kluwer Publishing, 2005.

A. Juels. “Technological Approaches to the RFID Privacy Problem.” S. Garfinkel and B. Rosenberg, eds., *RFID: Applications, Security, and Privacy*, pp. 329–338. Addison-Wesley, 2005.

A. Juels, ed., *Financial Cryptography, 8th International Conference (FC 2004)*, Key West, FL, USA, February 9–12, 2004, Revised Papers, Springer-Verlag, 2004. LNCS no. 3110.

A. Juels. “Encryption.” *Handbook of Information Security*, H. Bigdoli, ed., John Wiley & Sons, 2004.

A. Juels. “Encryption.” *The Internet Encyclopedia*, H. Bigdoli, ed., John Wiley & Sons, 2003.

## PROFESSIONAL SERVICE

**Steering Committee Member**, ACM SIGSAC, 2005–

**Associate Editor**, *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2008–

**Advisory Committee Member**, RSA Conference, 2008–

**Co-organizer**, RFID-CUSP Workshop, 2008

**General chair**, ACM Conference on Communications Security, 2006

**Program co-chair**, ACM Workshop on Wireless Security (WiSe ’06), 2006

**Vice Chair**, Security, Privacy, and Ethics Track, WWW2006: Fifteenth International World Wide Web Conference, 2006

**Program co-chair**, 3rd IEEE International Workshop on Pervasive Computing and Communication Security (PerSec), 2006

**Program chair**, ACM Conference on Communications Security, Industry Track, 2005

**Founding member**, Voting System Performance Rating (VSPR)

**Editorial board member**, *Handbook of Information Security*, 2005; *Handbook of Computer Networks*, 2006

**President**, International Financial Cryptography Association, 2004-2005

**Program chair**, 8th International Financial Cryptography Conference, 2004

**Program co-chair**, DIMACS Workshop on Electronic Voting, 2004

**Editorial board member**, *Internet Encyclopedia*, 2004

**Technical program committee memberships:**

- EUROCRYPT, 2010
- ACM Conference on Wireless Security (WiSec), 2009
- CRYPTO, 2008
- Secure Component and System Identification (SECSI), 2008
- International Workshop on RFID Data Management (RFDM), 2008
- IEEE Symposium on Security and Privacy (Oakland), 2008
- Applied Cryptography and Network Security (ACNS), 2008
- IAVoSS Workshop on Trustworthy Elections (WOTE), 2007
- 14th ACM Conference on Computer and Communications Security (ACM CCS), 2007
- 9th Information Security Conference (ISC), Pythagoras, Greece, 2006
- 10th International Financial Cryptography Conference (FC), 2006
- 12th Workshop on Selected Areas in Cryptography (SAC), 2005
- 3rd International Conference on Applied Cryptography and Network Security (ACNS), 2005
- 2nd International Conference on Security in Pervasive Computing (SPC), 2005
- ISOC Networks and Distributed Security Systems Symposium (NDSS), 2005
- Pervasive Computing and Communications Security Workshop (PerSec), 2005
- ACM Workshop on Wireless Security (WiSE), 2004
- 10th ACM Conference on Computer and Communications Security (ACM CCS), 2003
- 7th International Financial Cryptography Conference (FC), 2003
- Asiacrypt, 2002
- 9th ACM Conference on Computer and Communications Security (ACM CCS), 2002
- RSA Conference Cryptographers' Track (RSA-CT), 2001
- 5th ACM Conference on Computer and Communications Security (ACM CCS), 1999
- 3rd International Financial Cryptography Conference (FC), 1999
- ISOC Networks and Distributed Security Systems Symposium (NDSS), 1999
- ISOC Networks and Distributed Security Systems Symposium (NDSS), 1998

**Organizing committee memberships:** Organizer, RFID Privacy Workshop at MIT '03; Publicity chair, 8th ACM Conference on Computer and Communications Security (2001)

**Doctoral dissertation committees:** Philippe Golle, Ph.D., Stanford University, December 2003; Brent Waters, Ph.D., Princeton University, August 2004; Melanie Rieback, Ph.D., Vrije Universiteit, The Netherlands, September 2008

**Standards working group participation:** ANSI X9.F1 and X9.F4

**Government service:** NSF CyberTrust funding panel, June 2004; Numerous invited tutorials for USPTO examiners

## SELECTED MEDIA COVERAGE

*Boston Globe*, "RSA Labs scientist pens a tale of cybervillains," by Mark Baard. 20 July 2009. (Article about my thriller novel, *Tetraktys*.)

*CNET*, "Taking the Classical Approach to Security," by Vivian Yeo, 24 December 2008. (Interview on a range of topics.)

*Wall Street Journal*, "Border-Crossing Cards Can Be Copied," by Keith J. Winstein, 23 October 2008. (Article on joint Univ. of Washington/RSA Laboratories analysis of Passport Cards and Enhanced Drivers Licenses.)

*Forbes*, “In Pictures: Gadgets for Stopping Identity Theft,” by Andy Greenberg, 14 May 2008. (Coverage of RSA Labs’ handset-based access-control system.)

*ComputerWorld*, “40 Innovative IT People to Watch Under the Age of 40,” 9 July 2007.

*New York Times*, “Researchers See Pitfalls in No-Swipe Credit Cards,” by John Schwartz, 23 October 2006. (Article on joint UMass-Amherst/RSA Laboratories analysis of RFID-Enabled credit cards.)

*Consumer Reports*, “The End of Privacy?” by Andrea Rock, June 2006.

*Wired News*, “The RFID Hacking Underground,” by Annalee Newitz, 5 May 2006.

National Public Radio, *All Things Considered*, “High-Tech Passports Stir Controversy,” by Larry Abrahamson. 10 April 2005.

*New York Times*, “Graduate Cryptographers Unlock Code of ‘Thiefproof’ Car Key,” by John Schwartz. 29 January 2005. (Article on joint Johns Hopkins/RSA Labs reverse-engineering of cryptographic RFID device used in millions of payment tokens and automobile immobilizers.)

*Slashdot*, “Car RFID Security System Cracked.” 29 January 2005.

*Reuters*, “Auto, Gas Security Chips Vulnerable, Study Finds.” 29 January 2005.

*Technology Review*, “The 2004 TR100.” October 2004. List of the top 100 technology innovators in the world under 35 years of age. (Award is now called the TR35.)

National Public Radio, *Morning Edition*, “Radio Frequency IDs,” by Larry Abrahamson. (Discussion of co-invented RFID “blocker” tag and demonstration pharmacy.) 26 March 2004.

*Wired News*, “Jamming Tags Block RFID Scanners,” by Kim Zetter. 1 March 2004.

*Information Week*, “The closer RFID gets to consumers, the hotter privacy issues become,” by Thomas Claburn. 8 March 2004.

*The New Scientist*, “RFID blocker tags may soothe privacy fears,” by Celeste Biever. 26 February 2004.

*Slashdot*, “RSA Creating RFID Blocker Tag.” 24 February 2004.

*eWeek*, “RSA Keeps RFID Private,” by Dennis Fisher. 23 February 2004.

*Libération*, “La petite puce rapporteuse,” by Catherine Maussion. 31 May 2003. (French daily. Article on work on RFID in Euro banknotes and RFID privacy.)

*eWeek*, “RSA Seeks to Fix RFID Worries,” by Dennis Fisher. 25 August 2003.

*eWeek*, “RSA Looks to Lock Down Personal Data,” by Dennis Fisher. 14 April 2003. (Article on co-invented split-secret authentication system called Nightingale.)

## **SELECTED INVITED TALKS AND PANELS**

International Workshop on RFID Security and Cryptography 2009 (RISC). Keynote talk. November 2009.

FTC Workshop on Contactless Payment Technology. Panelist. October 2008.

WiSec, “RFID in the Shoulder and on the Loading Lock.” Keynote talk. March 2008.

DoD RFID Summit, “Practical Privacy and Security Solutions for RFID Implementations.” Panelist. April 2007.

Conference on Hardware and Embedded System Security (CHES), “The Outer Limits of RFID Security.” Keynote talk. October 2006.

ACM Workshop on Wireless Security, “RFID: Privacy and Security for Five-Cent Computers.” Invited talk. October 2004.

The Emerging Technologies Conference at MIT, “Fusion Biometrics.” Panelist. October 2004.

USENIX Security Conference, “RFID: Privacy and Security for Five-Cent Computers.” Invited talk. August 2004.

USENIX Technical Conference, “Wireless Devices and Consumer Privacy.” Panel organizer. June 2004.

U.S. Federal Trade Commission RFID Workshop. Panelist. June 2004.

U.S. Senate Judiciary Committee Staff Briefing. Panelist. June 2004.

U.S. Department of Commerce Wireless Sensor Technology Forum. Panelist. April 2004.

Stevens Symposium on Cybersecurity and Trustworthy Software, “RFID Tags: Privacy without Cryptography.” Invited talk. March 2004.

l’Ecole Normale Supérieure, “Squealing Euros: Privacy Protection in RFID-Enabled Banknotes” and “Nightingale: Distributed Cryptography for the Mass,” May and June 2003

M.I.T. Cryptography and Information Security Group. “Fuzzy Commitment.” Invited talk. September 2002.

Center for Applied Cryptographic Research (CACR) Security Symposium 2002, “Biometric Security.” Invited talk. May 2002.

United States Patent and Trademark Office, “Selected Topics in Cryptography.” Invited talk. June 2001.

ACM Computer and Communications Security, “Provable Security.” Panelist. November 1999.

Bell Laboratories, “Removing Paper-and-Pencil Metaphors from Cryptography.” Invited talk. June 1999.

Sandia National Laboratories, “New Directions in Digital Commerce.” Invited talk. November 1997.

## PATENTS

A. Juels. U.S. patent no. 7,532,104, “Low-complexity cryptographic techniques for use with radio frequency identification devices.” Issued 12 May 2009.

M. Jakobsson, A. Juels, and B. Kaliski. U.S. patent no. 7,502,933, “TIdentity authentication system and method.” Issued 10 March 2009 .

A. Juels. U.S. patent no. 7,472,093, “Targeted delivery of informational content with privacy protection.” Issued 30 Dec. 2008.

A. Juels et al. U.S. patent no. 7,461,399, “PIN recovery in a smart card.” Issued 2 Dec. 2008.

M. Jakobsson and A. Juels. U.S. patent no. 7,356,696 , “Proofs of work and bread pudding protocols.” Issued 8 Apr. 2008.

A. Juels and J. Brainard. U.S. patent no. 7,298,243 , “Radio frequency identification system with privacy policy implementation based on device classification.” Issued 20 November 2007.

A. Juels and N. Frykholm. U.S. patent no. 7,219,368, “Robust Visual Passwords.” Issued 15 May 2007.

A. Juels and J. Brainard. U.S. patent no. 7,197,639, “Cryptographic countermeasures against connection depletion attacks .” Issued 27 March 2007.

A. Juels, R. Rivest, and M. Szydlo. U.S. patent no. 6,970,070, “ Method and Apparatus for Selective Blocking of Radio Frequency Identification Devices.” Issued 29 Nov. 2005.

M. Jakobsson and A. Juels, U.S. patent no. 6,772,339, “Mix and Match: New Approach to Secure Multiparty Computation.” Issued 2 Nov. 2004.

M. Jakobsson and A. Juels, U.S. patent no. 6,813,354, “Mixing in Small Batches.” Issued 3 Aug. 2004.

A. Juels, U.S. patent no. 6,446,052, “Digital Coin Tracing Using Trustee Tokens.” Issued 3 Sept. 2002.

M. Liskov, B. Silverman, and A. Juels, U.S. patent no. 6,411,715, “Methods and Apparatus for Verifying the Cryptographic Security of a Selected Private and Public Key Pair Without Knowing the Private Key.” Issued 25 June 2002.

M. Jakobsson and A. Juels, U.S. patent no. 6,393,447, “Method and Apparatus for Extracting Unbiased Random Bits from a Potentially Biased Source of Randomness.” Issued 21 May 2002.

D. Huynh, M. Robshaw, A. Juels, and B. Kaliski, U.S. patent no. 6,240,184, “Password Synchronization.” Issued 29 May 2001.

M. Jakobsson and A. Juels, U.S. patent no. 6,157,920, “Executable Cash for Electronic Commerce.” Issued 5 Dec. 2000.

(Others pending.)

## FELLOWSHIPS and GRANTS

NASA Graduate Fellowship	1992-95
Pompeo Memorial Fellowship	1991-92
Amherst Memorial Fellowship	1991
Amherst Academy Fellowship	1991
Sloane Foundation Grant	1990
NSF Research Experience for Undergraduates Grant	1988

## OTHER EDUCATION AND HONORS

Visiting Researcher, l’ENS–Paris	1993-94
Visiting Scholar, Litterae Humaniores, Oxford University	1989-90
ComputerWorld, 40 IT Innovative IT People Under 40	2007
Outstanding Research Award in Privacy Enhancing Technologies	2007
IEEE, Best Tutorial Paper	2007
USENIX Security, Best Student Paper	2005
TR 100 (MIT <i>Technology Review</i> )	2004
Employee Excellence Award, RSA Security Inc.	1997
Bronze Medal, Northern California Foil Open	1996
MacKay Prize for Latin Verse Translation, U.C. Berkeley	1992
Phi Beta Kappa	1991
Frost Library Book Collecting Prize, Amherst College, Second Place	1991
Barry Goldwater Scholarship for Excellence in Science, First Alternate	1991
Novice Fencing Cup, First Prize, Oxford University	1990

Rex Warner Literary Prize, Wadham College, Oxford University	1990
Bertrand Latin Prize, Amherst College	1989