Ari Juels

55 Station Street, Apt. 3B
Brookline, MA 02445

E-mail: juels@cornell.edu
Web: www.arijuels.com

PROFESSIONAL EXPERIENCE

Professor	Cornell Tech Jacobs Cornell-Technion Institute	2014 –
Chief Scientist	RSA, The Security Division of EMC	2010 – 2013
Distinguished Engineer	EMC Corporation	2010 – 2013
Director	RSA Laboratories	2007 – 2013
Chief Scientist	RSA Laboratories	2007 – 2010
Principal Research Scientist	RSA Laboratories	1999 – 2007
Co-founder	RavenWhite Inc.	2005 – 2006
Senior Research Scientist	RSA Laboratories	1998 – 1999
Research Scientist	RSA Laboratories	1996 – 1998

RESEARCH AREAS

Cybersecurity, "big data" security analytics, user authentication, user privacy, cloud security, applied cryptography, medical device security, and RFID / NFC security

EDUCATION

Ph.D.	University of California at Berkeley Computer Science Division Dissertation: *Topics in Black-Box Combinatorial Optimization* Advisor: Prof. Alistair Sinclair	1991 – 1996
B.A.	Amherst College, Amherst, MA Latin Literature and Mathematics Phi Beta Kappa	1987 – 1991

CONFERENCE AND JOURNAL PUBLICATIONS

[MJSPK14] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz. PermaCoin: Repurposing Bitcoin Work for Long-Term Data Preservation. IEEE Symposium on Security and Privacy (S & P), 2014.

[JW14] A. Juels and B. Wong. Technical Perspective: Neuroscience Meets Cryptography. *Communications of the ACM* (CACM) 56(2): 64-73, May 2014.

[JR14] A. Juels and T. Ristenpart. Honey Encryption: Security Beyond the Brute-Force Bound. EUROCRYPT, pp. 293–310, 2014.

[YOOL+13] T.-F. Yen, A. Oprea, K. Onarlioglu, A. Juels, E. Kirda, and W. Robertson. Beehive: Large-Scale Log Analysis for Detecting Suspicious Activity in Enterprise Networks. Annual Computer Security Applications Conference (ACSAC), 2013.

[JR13a] A. Juels and R. L. Rivest. Honeywords: Making Password-Cracking Detectable. ACM Conference on Computer and Communication Security (ACM CCS), pp. 145–160, 2013.

[RJK13] M. Rostami, A. Juels, and F. Koushanfar. Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. ACM Conference on Computer and Communication Security (ACM CCS), pp. 1099–1112, 2013.

▷ *NYU-Poly Best Applied Security Paper Award, 2nd place.*

[RBJK13] M. Rostami, W. Burleson, A. Juels, and F. Koushanfar. Balancing Security and Utility in Medical Devices. ACM Design Automation Conference (DAC), Article no. 13, 2013.

[vDJOR13] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest. `FlipIt`: The Game of "Stealthy Takeover". *Journal of Cryptology* 26(4): 655–713, 2013.

[BJRS13] K. Bowers, A. Juels, R. Rivest, and E. Shen. Drifting Keys: Impersonation Detection for Constrained Devices. IEEE INFOCOM, pp. 1025–1033, 2013.

[AO13] A. Juels and A. Oprea. New Approaches to Security and Availability for Cloud Data. *Communications of the ACM* (CACM) 56(2): 64–73, February 2013.

[ZCJ13] D. Zanetti, S. Capkun, and A. Juels. Tailing RFID Tags for Clone Detection. Network and Distributed System Security Symposium (NDSS), 2013.

[SvDOJ12] E. Stefanov, M. van Dijk, A. Oprea, and A. Juels. Iris: A Scalable Cloud File System with Efficient Integrity Checks. Annual Computer Security Applications Conference (ACSAC), pp. 229–238, 2012.

▷ *NYU-Poly AT&T Best Applied Security Paper Award, 3rd place.*

[FVBJ+12] B. Farley, V. Varadarajan, K.D. Bowers, A. Juels, T. Ristenpart, M. Swift. More for Your Money: Exploiting Performance Heterogeneity in Public Clouds. Symposium on Cloud Computing (SOCC): 20, 2012.

[vDJOR+12] M. van Dijk, A. Juels, A. Oprea, R. L. Rivest, E. Stefanov, and N. Triandopoulos. Hourglass Schemes: How to Prove That Cloud Files Are Encrypted. ACM Conference on Computer and Communication Security (ACM CCS), pp. 265–280, 2012.

[YJRR12] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart. Cross-VM Side Channels and Their Use to Extract Private Keys. ACM Conference on Computer and Communication Security (ACM CCS), pp. 305–316, 2012.

[BvDGJ+12] K. D. Bowers, M. van Dijk, R. Griffin, A. Juels, A. Oprea, R. L. Rivest, and N. Triandopoulos. Defending against the Unknown Enemy: Applying `FlipIt` to System Security. Conference on Decision and Game Theory for Security (GameSec), pp. 248–263, 2012.

[JY12] A. Juels and T.F. Yen. Sherlock Holmes and the Case of the Advanced Persistent Threat. USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET): 2, 2012.

[BvDJO+12] K. Bowers, M. van Dijk, A. Juels, A. Oprea, and R. Rivest. How to Tell if Your Cloud Files Are Vulnerable to Drive Crashes. ACM Conference on Computer and Communication Security (ACM CCS), pp. 501–514, 2011.

[ZJOR11] Y. Zhang, A. Juels, A. Oprea, M. K. Reiter. HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis. IEEE Symposium on Security and Privacy (S & P), pp. 313–328, 2011.

[DBvDJ11] T. Denning, K. Bowers, M. van Dijk, and A. Juels. Exploring Implicit Memory for Painless Password Recovery. International Conference on Human Factors in Computing Systems (CHI), pp. 2615-2618, 2011.

[J10a] A. Juels. The Physical Basis of RFID Security. RFIDSec, p. 1, 2010. (Keynote abstract)

[OJ10] A. Oprea and A. Juels. A Clean-Slate Look at Disk Scrubbing. USENIX Conference on File and Storage Technologies (FAST), pp. 57–70, 2010.

[JvD10] M. van Dijk and A. Juels. On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing. USENIX Workshop on Hot Topics in Security (HotSec), 2010.

[JCJ10] A. Juels, D. Catalano, and M. Jakobsson. Coercion-Resistant Electronic Elections. In Chaum et al., eds., *Towards Trustworthy Elections*, pp. 37–63, 2010. (Workshop version appeared as [JCJ05].)

[JJ09] M. Jakobsson and A. Juels. Server-Side Detection of Malware Infection. New Security Paradigms Workshop (NSPW), pp. 11–22, 2009.

[JW09] A. Juels and S. Weis. Defining Strong Privacy for RFID. *ACM Transactions on Information and System Security* (TISSEC) 13(1), article no. 7, October 2009.

[KJKB09] K. Koscher, A. Juels, T. Kohno, and V. Brajkovic. EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. ACM Conference on Computer and Communication Security (ACM CCS), pp. 187–198, 2009.

[BJO09a] K. Bowers, A. Juels, and A. Oprea. HAIL: A High-Availability and Integrity Layer for Cloud Storage. ACM Conference on Computer and Communication Security (ACM CCS), pp. 187–198, 2009.

[SCRF+09] M. Salajegheh, S. Clark, B. Ransford, K. Fu, and A. Juels. CCCP: Secure Remote Storage for Computational RFIDs. USENIX Security Symposium, pp. 215–230, 2009.

[BJO09b] K. Bowers, A. Juels, and A. Oprea. Proofs of Retrievability: Theory and Implementation. ACM Cloud Computing Security Workshop (CCSW), pp. 43–54, 2009.

[JPP08] A. Juels, B. Parno, and R. Pappu. Unidirectional Key Distribution Across Time and Space with Applications to RFID Security. USENIX Security Symposium, pp. 75-90, 2008.

[J08] A. Juels. RFID security: in the shoulder and on the loading dock. ACM conference on Wireless network security (WiSec), p.1, 2008. (Abstract of keynote talk.)

[JJR08] M. Jakobsson, A. Juels, and Jacob Ratkiewicz. Privacy-Preserving History Mining for Web Browsers. W2SP, 2008.

[CEJM+07] S.G. Choi, A. Elbaz, A. Juels, T. Malkin, and M. Yung. Two-Party Computing with Encrypted Data. Advances in Cryptology–ASIACRYPT, pp. 298–314, 2007.

[BBGJ07] D. Bailey, D. Boneh, E.-J. Goh, and A. Juels. Covert Channels in Privacy-Preserving Identification Systems. ACM Conference on Computer and Communications Security (ACM CCS), pp. 297–306, 2007.

[JK07] A. Juels and B. Kaliski. PORs: Proofs of Retrievability for Large Files. ACM Conference on Computer and Communications Security (ACM CCS), pp. 584–597, 2007.

[HBFJ+07] T. Heydt-Benjamin, D. Bailey, K. Fu, A. Juels, and T. O'Hare. Vulnerabilities in First-Generation RFID-Enabled Credit Cards. Financial Cryptography and Data Security, pp. 2–14, 2007.

[BFJ07] B. Defend, K. Fu, and A. Juels. Cryptanalysis of Two Lightweight RFID Authentication Schemes. Percom Workshops (PerSec), pp. 211–216, 2007.

[JW07] A. Juels and S. Weis. Defining Strong Privacy for RFID. PerCom Workshops (PerTec), pp. 342–347, 2007.

[JSJ07] A. Juels, S. Stamm, and M. Jakobsson. Combating Click Fraud via Premium Clicks. USENIX Security Symposium, pp. 17–26, 2007.

[BJRS+06] J. Brainard, A. Juels, R. Rivest, M. Szydlo, and M. Yung. Fourth-Factor Authentication:

Someone You Know. ACM Conference on Computer and Communications Security (ACM CCS), pp. 168–178, 2006.

[BJ06] D. Bailey and A. Juels. Shoehorning Security into the EPC Standards. Security and Cryptography for Networks (SCN), pp. 303–320, 2006.

[HJSW06] 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.

[JJJ06] A. Juels, M. Jakobsson, and T. Jagatic. Cache Cookies for Browser Authentication (Extended Abstract). IEEE Symposium on Security and Privacy, pp. 301–305, 2006.

[J06a] A. Juels. RFID Security and Privacy: A Research Survey. *Journal of Selected Areas in Communication (J-SAC)*, 24(2):381–395, February 2006.
▷ *2007 IEEE Best Tutorial Paper Award.*

[JS06] A. Juels and M. Sudan. A Fuzzy Vault Scheme. *Designs, Codes, and Cryptography*, 38(2): 237 – 257, February 2006. (One-page abstract appeared as [JS02].)

[J06b] A. Juels: The Outer Limits of RFID Security. Cryptographic Hardware and Embedded Systems (CHES), p. 231, 2006. (Abstract of invited talk.)

[JMW05] A. Juels, D. Molnar, and D. Wagner. Security and Privacy Issues in E-passports. SecureComm, pp. 74–88, 2005.

[JW05] A. Juels and S. Weis. Authenticating Pervasive Devices with Human Protocols. Advances in Cryptology–CRYPTO, pp. 293–308, 2005.

[J05d] A. Juels. Strengthening EPC Tags Against Cloning. ACM Workshop on Wireless Security (WiSec), pp. 67–76, 2005.

[JSB05] A. Juels, P. Syverson, and D. Bailey. High-Power Proxies for Enhancing RFID Privacy and Utility. Workshop on Privacy Enhancing Technologies (WPES), pp. 210–226, 2005.

[BGSJ+05] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security Analysis of the a Cryptographically Enabled RFID Device. USENIX Security Symposium, pp. 1–16, 2005.
▷ *Best Student Paper Award, USENIX Security*
▷ *Outstanding Research Award in Privacy Enhancing Technologies (2007)*

[JRG05] S. Garfinkel, A. Juels, and R. Pappu. RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy*, 3(3): 34–43. May/June 2005.

[JCJ05] A. Juels, D. Catalano, and M. Jakobsson. Coercion-Resistant Electronic Elections. *Workshop on Privacy in the Electronic Society* (WPES), pp. 61–70, 2005.

[J04b] A. Juels. Minimalist Cryptography for RFID Tags. Security of Communication Networks (SCN), pp. 149–164, 2004.

[JB04] A. Juels and J. Brainard. Soft Blocking: Flexible Blocker Tags on the Cheap. Workshop on Privacy Enhancing Technologies (WPES), pp. 1–7, 2004.

[WJHF04] B. Waters, A. Juels, A. Halderman, and E. Felten. New Client Puzzle Outsourcing Techniques for DoS Resistance. ACM Conference on Computer and Communications Security (ACM CCS), pp. 246–256, 2004.

[GJ04a] P. Golle and A. Juels. Parallel Mixing. ACM Conference on Computer and Communications Security (ACM CCS), pp. 220–226, 2004.

[GJ04b] P. Golle and A. Juels. Dining Cryptographers Revisited. Advances in Cryptology–EUROCRYPT, pp. 456–473, 2004.

[J04c] A. Juels. "Yoking-Proofs" for RFID Tags. IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW), pp.138–143, 2004.

[J04d] A. Juels. RFID: security and privacy for five-cent wireless devices. Workshop on Wireless Security (WiSec), p. 31, 2004. (Abstract of keynote talk.)

[J04e] A. Juels. RFID: Security and Privacy for Five-Cent Computers. USENIX Security Symposium. (Abstract of invited talk.)

[GJJS04] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal Re-Encryption for Mixnets. RSA Conference Cryptographers' Track (CT-RSA), pp. 163–178, 2004.

[JRS03] A. Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. ACM Conference on Computer and Communications Security (ACM CCS), pp. 103–111, 2003.

[BJKS03] J. Brainard, A. Juels, B. Kaliski, and M. Szydlo. A New Two-Server Approach for Authentication with Short Secrets. USENIX Security Symposium, pp. 201–214, 2003.

[JP03] A. Juels and R. Pappu. Squealing Euros: Privacy-Protection in RFID-Enabled Banknotes. Financial Cryptography, pp. 103–121, 2003.

[JS02] A. Juels and M. Sudan. A Fuzzy Vault Scheme. International Symposium on Information Theory (ISIT), p. 408, 2002.

[GZBJ+02] P. Golle, S. Zhong, D. Boneh, M. Jakobsson, and A. Juels. Optimistic Mixing for Exit Polls. Advances in Cryptology–ASIACRYPT, pp. 451–465, 2002.

[JG02] A. Juels and J. Guajardo. RSA Key Generation with Verifiable Randomness. Public Key Cryptography (PKC), pp. 357–374, 2002.

[JJR02] M. Jakobsson, A. Juels, and R. L. Rivest. Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking. USENIX Security Symposium, pp. 339–353, 2002.

[JS02b] A. Juels and M. Szydlo. A Two-Server Auction Protocol. Financial Cryptography (FC), pp. 72–86, 2002.

[JJN02] M. Jakobsson, A. Juels, and P. Q. Nguyen. Proprietary Certificates. RSA Conference Cryptographers' Track (CT-RSA), pp. 164–181, 2001.

[JJ01] M. Jakobsson and A. Juels. An Optimally Robust Hybrid Mix Network. ACM Symposium on Principles of Distributed Computing (PODC), pp. 284–292, 2001.

[FJ01] N. Frykholm and A. Juels. Error-Tolerant Password Recovery. ACM Conference on Computer and Communications Security (ACM CCS), pp. 1–9, 2001.

[J01] A. Juels. Targeted Advertising... and Privacy Too. RSA Conference Cryptographers' Track (CT-RSA), pp. 408–424, 2001.

[JJ00a] M. Jakobsson and A. Juels. Mix and Match: Secure Function Evaluation via Ciphertexts. Advances in Cryptology – ASIACRYPT, pp. 346–358, 2000.

[JJ00b] M. Jakobsson and A. Juels. Addition of El Gamal Plaintexts, Advances in Cryptology – ASIACRYPT, pp. 346–358, 2000.

[HJJY00] J. Håstad, J. Jonsson, A. Juels, and M. Yung, Funkspiel Schemes: An Alternative to Conventional

Tamper Resistance. ACM Conference on Computer and Communications Security (ACM CCS), pp. 125–133, 2000.

[JJSH00] A. Juels, M. Jakobsson, E. Shriver, and B. Hillyer. How to Turn Loaded Dice into Fair Coins. *IEEE Transactions on Information Theory* 46 (3): 911–921, May 2000.

[JP00] A. Juels and M. Peinado. Hiding Cliques for Cryptographic Security. *Designs, Codes, and Cryptography*, 20(3):269–280, July 2000. (Conference version in ACM-SIAM Symposium on Discrete Algorithms (SODA), 1998.)

[JW99] A. Juels and M. Wattenberg. A Fuzzy Commitment Scheme. ACM Conference on Computer and Communications Security (ACM CCS), pp. 28–36, 1999.

[JJ99a] M. Jakobsson and A. Juels. Proofs of Work and Bread Pudding Protocols. Communications and Multimedia Security, pp. 258–272, 1999.

[JB99] A. Juels and J. Brainard. Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks. Network and Distributed System Security Symposium (NDSS), pp. 151–165, 1999.

[J99] A. Juels. Trustee Tokens: Simple and Practical Tracing of Anonymous Digital Cash. Financial Cryptography (FC), pp. 29–45, 1999.

[JSHJ98] M. Jakobsson, L. Shriver, B. Hillyer, and A. Juels. A Practical Secure Physical Random Bit Generator. ACM Conference on Computer and Communications Security (ACM CCS), pp. 103–111, 1998.

[JJ98] M. Jakobsson and A. Juels. X-cash: Executable Digital Cash. Financial Cryptography (FC), pp. 16–27, 1998.

[JLO97] A. Juels, M. Luby, and R. Ostrovsky. Security of Blind Digital Signatures. Advances in Cryptology – CRYPTO, pp. 150–164, 1997.

[JW95] A. Juels and M. Wattenberg. Hillclimbing as a Baseline Method for the Evaluation of Stochastic Optimization Algorithms. Advances in Neural Information Processing Systems (NIPS), pp. 430–436, 1995.

BOOK CHAPTERS / EDITED VOLUMES / GUEST ARTICLES

[JR13b] A. Juels and R. L. Rivest. For Stronger Password Security, Try a Spoonful of Honeywords. *Wired*. Innovation Insights. 8 May 2013.

[J10b] A. Juels. Future Tense: The Primal Cue. *Communications of the ACM (CACM)*, 53(3):120–ff, Mar. 2010.

[J09] A. Juels. How 10 digits will end privacy as we know it. *CNET*. Guest column. 17 August 2009.

[K08] T. Kohno. An Interview with RFID Security Expert Ari Juels. IEEE Pervasive Computing, 7(1):10–11, 2008.

[J07] A. Juels. The Vision of Secure RFID. *Proceedings of the IEEE*, 95(8):1–2, August 2007.

[JWdCdV06] A. Juels, R. N. Wright, and S. De Capitani di Vimercati, eds., *13th ACM Conference on Computer and Communications Security*, ACM Press, 2006.

[J06c] A. Juels. "The Limitations of Perfect User Authentication." *Phishing and Anti-Phishing*, M. Jakobsson and S. Myers, eds., John Wiley & Sons, 2006.

[J06d] A. Juels. "Cryptography." *Handbook of Computer Networks*, H. Bigdoli, ed., John Wiley & Sons, 2006.

[AMJ05] V. Atluri, C. Meadows, and A. Juels, eds., *12th ACM Conference on Computer and Communications Security*, ACM Press, 2005.

[J05e] A. Juels. A Bit of Privacy. In *RFID Journal*, 2 May 2005. Guest column.

[J05f] A. Juels. Attack on a Cryptographic RFID Device. In *RFID Journal*, 28 Feb. 2005. Guest column.

[J05g] A. Juels. "RFID Privacy: A Technical Primer for the Non-Technical Reader." *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. Kluwer Publishing, 2005.

[J05h] 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.

[J04f] 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.

[J04g] A. Juels. "Encryption." *Handbook of Information Security*, H. Bigdoli, ed., J. Wiley & Sons, 2004.

[J03] A. Juels. "Encryption." *The Internet Encyclopedia*, H. Bigdoli, ed., John Wiley & Sons, 2003.

BOOKS

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

ISSUED PATENTS

E. Stefanov, M. van Dijk, A. Oprea, and A. Juels. Scalable cloud file system with efficient integrity checks. U.S. patent 8,706,701. Issued 22 April 2014.

A. Juels. Forward-secure key unlocking for cryptographic devices. U.S. patent 8,700,899. Issued 15 April 2014.

A. Juels, J. G. Brainard, and R. D. Hopley. On-demand proactive epoch control for cryptographic devices. U.S. patent 8,699,715. Issued 15 April 2014.

A. Juels and R. L. Rivest. Key update with compromise detection. U.S. patent 8,699,713. Issued 15 April 2014.

A. Oprea, Y. Zhang, V. Ganti, J. P. Field, A. Juels, and M.K. Reiter. Security policy enforcement framework for cloud-based information processing systems. U.S. patent 8,689,282. Issued 1 April 2014.

M. van Dijk, K. D. Bowers, S. Curry, S. P. Doyle, W. M. Duane, A. Juels, M. J. O'Malley, N. Triandopoulos, and R. Zolfonoon. Soft token posture assessment. U.S. patent 8,683,563. Issued 25 March 2014.

A. Juels and A. Oprea. Counter-based encryption of stored data blocks. U.S. patent 8,635,465. Issued 21 January 2014.

K. Bowers, T. Denning, and A. Juels. Methods and apparatus for authenticating a user based on implicit user memory. U.S. patent 8,627,421. Issued 7 January 2014.

M. van Dijk, A. Juels, B.W. Fitzgerald, and G. Matthews. "Providing a security-sensitive environment ." U.S. patent 8,621,649. Issued 31 December 2013.

D. V. Bailey, J. Brainard, A. Juels, and K.D. Bowers. "Radio frequency identification enabled mobile device." U.S. patent 8,618,913. Issued 31 December 2013.

K. D. Bowers and A. Juels. "Personal Identification Pairs." U.S. patent 8,601,552. Issued 3 December 2013.

B.M. Jakobsson and A. Juels. "Method and apparatus for storing information in a browser storage area of

a client device." U.S. patent 8,533,350. Issued 10 September 2013.

A. Juels. "Method and system for preventing de-duplication side-channel attacks in cloud storage systems." U.S. patent 8,528,085. Issued 3 September 2013.

A. Juels and D. V. Bailey. "Access Control for Implanted Medical Devices." U.S. patent 8,515,070. Issued 20 August 2013.

A. Juels, O. Krieger, and D. Moreau. "Refresh-and-Rotation Process for Minimizing Resource Vulnerability to Workloads." U.S. patent 8,505,097. Issued 6 August 2013.

A. Juels and D. V. Bailey. "Device-based password management." U.S. patent 8,499,157. Issued 30 July 2013.

D. V. Bailey, J. G. Brainard, A. Juels, and B.S. Kaliski, Jr. "Authentication methods and apparatus using pairing protocols and other techniques." U.S. patent 8,495,372. Issued 23 July 2013.

D. V. Bailey, M. Ciaffi, W. Duane, A. Juels, and J. O'Brien. "Techniques for message-passing using shared memory of an RF tag". U.S. patent 8,458,483. Issued 4 June 2013.

J. G. Brainard, A. Juels, R. L. Rivest, and M. Szydlo. "User authentication based on voucher codes." U.S. patent 8,438,617. Issued 7 May 2013.

A. Juels, B. S. Kaliski, K.D. Bowers, and A. M. Oprea. "Proof of retrievability for archived files." U.S. patent 8,381,062. Issued 5 May 2013.

D. V. Bailey and A. Juels. "Security provision in standards-compliant RFID systems." U.S. patent 8,378,786. Issued 19 Feb. 2013.

A. Juels, M. van Dijk, A. M. Oprea, R. L. Rivest, and E. Stefanov. "Remote verification of file protections for cloud data storage." U.S. patent 8,346,742. Issued 1 Jan. 2013.

K.D. Bowers and A. Juels and A. M. Oprea. "Distributed storage system with enhanced security ." U.S. patent 8,132,073. Issued 6 Mar. 2012.

A. Juels and B. Parno. "Key distribution in unidirectional channels with applications to RFID." U.S. patent 8,031,875. Issued 4 Oct. 2011.

A. Juels, D.V. Bailey, and P. Syverson. "Proxy device for enhanced privacy in an RFID system." U.S. patent 7,920,050. Issued 5 Apr. 2011.

A. Juels. "Authentication methods and apparatus utilizing hash chains." U.S. patent 7,848,746. Issued 7 Dec. 2010.

A. Juels. "Methods and apparatus for RFID device authentication." U.S. patent 7,750,793. Issued 6 July 2010.

A. Juels and B. Kaliski. "Cryptographic methods and apparatus for secure authentication." U.S. patent 7,725,730. Issued 25 May 2010.

A. Juels. "Order invariant fuzzy commitment system." U.S. patent 7,602,904. Issued 13 Oct. 2009.

A. Juels. "Low-complexity cryptographic techniques for use with radio frequency identification devices." U.S. patent 7,532,104. Issued 12 May 2009.

M. Jakobsson, A. Juels, and B. Kaliski. "Identity authentication system and method." U.S. patent 7,502,933. Issued 10 Mar. 2009.

A. Juels. "Targeted delivery of informational content with privacy protection." U.S. patent 7,472,093. Issued

30 Dec. 2008.

A. Juels et al. "PIN recovery in a smart card." U.S. patent 7,461,399. Issued 2 Dec. 2008.

M. Jakobsson and A. Juels. "Proofs of work and bread pudding protocols." U.S. patent 7,356,696. Issued 8 Apr. 2008.

A. Juels and J. Brainard. "Radio frequency identification system with privacy policy implementation based on device classification." U.S. patent 7,298,243. Issued 20 November 2007.

A. Juels and N. Frykholm. "Robust Visual Passwords." U.S. patent 7,219,368. Issued 15 May 2007.

A. Juels and J. Brainard. "Cryptographic countermeasures against connection depletion attacks." U.S. patent 7,197,639. Issued 27 March 2007.

A. Juels, R. Rivest, and M. Szydlo. " Method and Apparatus for Selective Blocking of Radio Frequency Identification Devices." U.S. patent 6,772,339. Issued 29 Nov. 2005.

M. Jakobsson and A. Juels. "Mix and Match: New Approach to Secure Multiparty Computation." U.S. patent 6,772,339. Issued 2 Nov. 2004.

M. Jakobsson and A. Juels. "Mixing in Small Batches." U.S. patent 6,813,354. Issued 3 Aug. 2004.

A. Juels. "Digital Coin Tracing Using Trustee Tokens." U.S. patent 6,446,052. Issued 3 Sept. 2002.

M. Liskov, B. Silverman, and A. Juels. "Methods and Apparatus for Verifying the Cryptographic Security of a Selected Private and Public Key Pair Without Knowing the Private Key." U.S. patent 6,411,715. Issued 25 June 2002.

M. Jakobsson and A. Juels. "Method and Apparatus for Extracting Unbiased Random Bits from a Potentially Biased Source of Randomness." U.S. patent 6,393,447. Issued 21 May 2002.

D. Huynh, M. Robshaw, A. Juels, and B. Kaliski. "Password Synchronization." U.S. patent 6,240,184. Issued 29 May 2001.

M. Jakobsson and A. Juels. "Executable Cash for Electronic Commerce." U.S. patent 6,157,920. Issued 5 Dec. 2000.

(55+ patents pending)

SELECTED MEDIA COVERAGE

New Scientist. "The Bitcoin Spin-Off Currency That's Also an Archive," by Aviva Rutkin, 12 June 2014. (Coverage of Permacoin.)

Slashdot, "Building Deception Into Encryption Software," 29 January 2014. (Coverage of "honey encryption" research.)

MIT Technology Review, "'Honey Encryption' Will Bamboozle Attackers with Fake Secrets," by Tom Simonite, 29 January 2014. (Article on "honey encryption" research.)

Forbes, "Security That Keeps Medical Implants Safe from Hackers," by Taylor Kubota. 23 October 2013. (Article on joint Rice Univ. / RSA Labs research on medical-device security.)

Wall Street Journal, "A Password for Implants," by Daniel Akst. 4 Oct. 2013. (Article on joint Rice Univ. / RSA Labs research on medical-device security.)

Slashdot, "Honeywords: Honeypot Passwords," 8 May 2013. (Coverage of "honeywords" research paper.)

NBCNews, "Fake 'honeyword' passwords could be planted to trip up hackers." 7 May 2013. (Article on "honeywords" research paper.)

Slashdot, "Attack Steals Crypto Key From Co-Located Virtual Machines," 6 November 2012. (Coverage of joint Univ. of North Carolina / RSA Labs / Univ. of Wisconsin research on cloud security.)

MIT Technology Review, "How to Steal Data from Your Neighbor in the Cloud," by Tom Simonite, 8 November 2012. (Article on joint Univ. of North Carolina / RSA Labs / Univ. of Wisconsin research on cloud security.)

MIT Technology Review, "To Keep Passwords Safe from Hackers, Just Break Them into Bits," by Tom Simonite, 9 October 2012. (Article on RSA product developed by RSA Labs.)

New Scientist, "RFID tags get an intelligence upgrade," by Kurt Kleiner, 14 August 2009. (Article on joint UMass / RSA Labs work on computational RFID tags.)

Slashdot, "Book Reviews: *Tetraktys*," 29 July 2009. (Review of my thriller novel *Tetraktys*.)

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 with me on a range of topics.)

Slashdot, "Researchers Find Problems With RFID Passport Cards." 24 October 2008. (Coverage of joint Univ. of Washington/RSA Laboratories analysis of Passport Cards and Enhanced Drivers Licenses.)

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.)

New York Times, "Researchers find problems with RFID passport cards," by Stephen Lawson. 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, "The RFID Hacking Underground," by Annalee Newitz, 5 May 2006. (Article on RFID security community work, including my research.)

National Public Radio, *All Things Considered*, "High-Tech Passports Stir Concerns," by Larry Abramson. 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 many payment tokens and automobile immobilizers.)

Slashdot, "Car RFID Security System Cracked." 29 January 2005. (Coverage of joint Johns Hopkins/RSA Labs reverse-engineering of cryptographic RFID device used in many payment tokens and automobile immobilizers.)

MIT 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 Abramson. (Discussion of co-invented RFID "blocker" tag and demonstration pharmacy.) 26 March 2004.

Slashdot, "RSA Creating RFID Blocker Tag." 24 February 2004. (Coverage of co-invented RFID "blocker" tag.)

PROFESSIONAL SERVICE

Co-organizer, DIMACS Workshop on Secure Cloud Computing, March 2014

Project Advisory Committee member, Strategic Healthcare IT Advanced Research Projects on Security (SHARPS), 2010-2014

Academic Advisory Board member, MIT Consortium for Kerberos and Internet Trust, 2013-

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; Davide Zanetti, Ph.D., ETH Zurich, December 2012; Masoud Rostami, Rice Univ., May 2014; Yinqian Zhang, UNC, June 2014

Program co-chair, CCSW, 2013

Program co-chair, RFIDSec, 2011

Steering Committee Member, ACM SIGSAC, 2005–09

Associate Editor, **IEEE Transactions on Dependable and Secure Computing (TDSC)**, 2008–10

Advisory Committee Member, RSA Conference, 2008–2012

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 participation: IEEE S&P , 2015; NDSS, 2014; IEEE S&P , 2014; ACM CCS, 2013; CRYPTO, 2012; NDSS, 2012; ACM CCS, 2010; EUROCRYPT, 2010; WiSec, 2009; CRYPTO, 2008; IEEE S&P, 2008; ACNS, 2008; WOTE, 2007; ACM CCS, 2007; ISC (Pythagoras), 2006; FC, 2006; SAC, 2005; ACNS, 2005; SPC, 2005; NDSS, 2005; PerSec, 2005; WiSE, 2004; ACM CCS, 2003; FC, 2003; Asiacrypt, 2002; ACM CCS, 2002; CT-RSA, 2001; ACM CCS, 1999; FC, 1999; NDSS, 1999; NDSS, 1998

Organizing committee memberships: Organizer, RFID Privacy Workshop at MIT '03; Publicity chair, ACM CCS, 2001

Creator, RSA Conference Cryptographers' Track (CT-RSA)

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

Government bodies: FCC Technical Advisory Board, 2010–11, Numerous invited tutorials for USPTO examiners

SELECTED INVITED TALKS AND PANELS

ACM SACMAT. Keynote talk. June 2014.

EPFL Summer Research Institute. Invited talk. June 2014.

Google-UMD Cybersecurity Seminar Series. Invited Talk. March 2013.

RSA Conference Cryptographers' Panel. Moderator. February 2013.

SecureCloud. Invited talk. May 2012.

RSA Conference Cryptographers' Panel. Moderator. March 2012.

Schloss Dagstuhl joint seminar on cloud security. Keynote talk. December 2011.

RSA Conference Cryptographers' Panel. Moderator. March 2011.

EPFL Summer Research Institute. Invited talk. June 2010.

RFIDSec. Keynote talk. June 2010.

RSA Conference Cryptographers' Panel. Moderator. March 2010.

International Workshop on RFID Security and Cryptography (RISC), "Power Games in RFID Security." Keynote talk. November 2009.

RSA Conference Cryptographers' Panel. Moderator. April 2009.

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

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

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

USENIX Security, "RFID: Privacy and Security for Five-Cent Computers." Invited talk. August 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.

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 Infosec Group. "Fuzzy Commitment." Invited talk. September 2002.

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

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

GRANT

National Science Foundation (NSF) TWC: Frontier: Collaborative: Rethinking Security in the Era of Cloud Computing, 2013–2018. $5.8 million multidisciplinary grant with nine co-PIs. (As an industry participant at submission, I am an unfunded co-PI.)

AWARDS

NYU-Poly Best Applied Security Paper Award [renamed after 2012], 2nd place	2013
NYU-Poly AT&T Applied Security Paper Award, 3rd Place	2012
EMC Innovation Showcase, 2nd Place	2011
ComputerWorld, 40 IT Innovative IT People Under 40	2007
PET Award for Outstanding Research in Privacy Enhancing Technologies	2007
Best Tutorial Paper Award, IEEE Communications Society	2007
Best Student Paper, USENIX Security	2005
TR 100 (MIT *Technology Review*), "100 remarkable innovators under the age of 35." (Now called TR35)	2004