Ari Juels

Cornell Tech
2 West Loop Road
New York, NY 10044

E-mail: juels@cornell.edu
Homepage: http://www.arijuels.com

Citizenship: U.S.A.

Current Positions

Weill Family Foundation and Joan and Sanford I. Weill Professor, Jacobs Technion-Cornell Institute, Cornell Tech	2019 – present
Co-Director, Initiative for CryptoCurrencies and Contracts (IC3)	2016 – present
Chief Scientist, Chainlink	2020 – present

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

Appointments Held

Professor	Jacobs Technion-Cornell Institute, Cornell Tech	2014 – 2019
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

Teaching and Advising

Courses

- *CS 5094, Blockchains, Cryptocurrencies, and Smart Contracts.* Cornell University (Cornell Tech), Spring 2017, Spring 2018.
- *CS 5433 Blockchains, Cryptocurrencies, and Smart Contracts.* Cornell University (Cornell Tech), Spring 2018, Spring 2020.
- *CS 5435, Security and Privacy Concepts in the Wild.* Cornell University (Cornell Tech), Fall 2014, Fall 2015, Fall 2016, Fall 2017.
- *CS 5438, Security and Privacy: Practice and Case Studies.* Cornell University (Cornell Tech), Spring 2016. (Co-taught with Vitaly Shmatikov)
- *CS 6431, Security and Privacy Technologies.* Cornell University, Fall 2015, Fall 2016. (Co-taught with Thomas Ristenpart and Vitaly Shmatikov)
- *CS 6466 Blockchains, Cryptocurrencies, and Smart Contracts.* Cornell University, Fall 2019.
- *CS 7435, Special Topics in Applied Security and Privacy.* Cornell University, Spring 2016.

Current Ph.D. Students

- Kushal Babel
- Philip Daian
- Yan Ji
- Sishan Long
- Mahimna Kelkar
- (Sai Krishna) Deepak Maram

Current Postdoctoral Mentees

- Steven Goldfeder (IC3 postdoc, co-mentored with Andrew Miller)

Former PhD students

- Ethan Cecchetti (co-advised with Andrew Myers) (Postdoc, UMD, 2021-)
- Fan Zhang (Duke University, 2021-)

Former Postdoctoral Mentees

- Ian Miers (IC3 postdoc, co-mentored with Tom Ristenpart), 2017-19
- Hussam Abu-Libdeh (Jacobs Runway Postdoc), 2014-15

Selected Honors

- Test of Time Award (for 1999 "Client Puzzles" paper), NDSS, 2019
- Faculty Teaching Award, Cornell Tech, 2018
- Distinguished Student Paper Award, IEEE S&P, 2016
- IBM Faculty Research Award, 2016
- Google Faculty Research Award, 2015
- Distinguished Student Paper Award, IEEE S&P, 2015
- Cisco Internet of Things Security Grand Challenge, Winner, 2014
- 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 Winner, 2nd Place, 2011
- International Book Awards, Winner, Fiction: Mystery and Suspense (for *Tetraktys*), 2010
- ComputerWorld, 40 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
- NASA Graduate Fellowship, 1992–95
- Pompeo Memorial Fellowship, 1991–92
- Amherst Memorial Fellowship, 1991
- Amherst Academy Fellowship, 1991

Publications

Publications in Reviewed Proceedings

[MMZJ-L+21] D. Maram, H. Malvai, F. Zhang, N. Jean-Louis, A. Frolov, T. Kell, T. Lobban, C. Moy, A. Juels, and A. Miller. CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability. IEEE S&P, 2021.

[HZJD+21] C. Hou, M. Zhou, Y. Ji, P. Daian, F. Tramer, G. Fanti, and A. Juels. SquirRL: Automating Attack Discovery on Blockchain Incentive Mechanisms with Deep Reinforcement Learning. NDSS 2021.

[ACEF+20] S. Allen, S. Capkun, I. Eyal, G. Fanti, B. Ford, J. Grimmelmann, A. Juels, K. Kostianinen, S. Meiklejohn, A. Miller, E. Prasad, K. Wüst, and F. Zhang. Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. 2020.

[KZGJ20] M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels. Order-Fairness for Byzantine Consensus. CRYPTO, pp. 451–480, 2020.

[MJPK-M+20] M. Mirkin, Y. Ji, J. Pang, A. Klages-Mundt, I. Eyal, and A. Juels. BDoS: Blockchain Denial of Service. ACM CCS, 2020. To appear.

[ZMMG+20] F. Zhang, S. K. D. Maram, H. Malvai, S. Goldfeder, and A. Juels. DECO: Liberating Web Data Using Decentralized Oracles for TLS. ACM CCS, 2020. To appear. Project website: deco.works.

[DGKL+20] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. IEEE S&P, 2020.

[ZDBJ19] F. Zhang, P. Daian, I. Bentov, and A. Juels. Paralysis Proofs: Safe Access-Structure Updates for Cryptocurrencies and More. Advances in Financial Technologies (AFT), 2019.

[CMJ+19] E. Cecchetti, B. Fisch, I. Miers, and A. Juels. PIEs: Public Incompressible Encodings for Decentralized Storage. ACM CCS, pp. 1351-1367, 2019.

[CRCM+19] R. Chatterjee, M. S. Riazi, T. Chowdhury, E. Marasco, F. Koushanfar, and A. Juels. Multisketches: Practical Secure Sketches Using Off-the-Shelf Biometric Matching Algorithms. ACM CCS, pp. 1171-1186, 2019.

[BJZB+19] I. Bentov, Y. Ji, F. Zhang, L. Breidenbach, P. Daian, and A. Juels. Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware. ACM CCS, pp. 1521-1538, 2019.

[MZWL+19] S.K.D. Maram, F.. Zhang, L. Wang, A. Low, Y. Zhang, A. Juels, and D. Song. CHURP: Dynamic-Committee Proactive Secret Sharing. ACM CCS, pp. 2369-2386, 2019.

[CZKH+19] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song. Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution. To appear in Euro S&P, 2019.

[BDTJ18] L. Breidenbach, P. Daian, F. Tramèr, and A. Juels. Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts. USENIX Security, 2018.

[SSMAC18] S. Matetic, M. Schneider, A. Miller, A, Juels, and S. Capkun. DelegaTEE: Brokered Delegation Using Trusted Execution Environments. USENIX Security, 2018.

[CZJK+17] E. Cecchetti, F. Zhang, Y. Ji, A. Kosba, A. Juels, and E. Shi. Solidus: Confidential Distributed Ledger Transactions via PVORM. ACM CCS, pp. 701-717, 2017.

[WCHJ+17] J. Woodage, R. Chatterjee, Y. Dodis, A. Juels, and T. Ristenpart. A New Distribution-Sensitive Secure Sketch and Popularity-Proportional Hashing. CRYPTO, pp. 682-710, 2017.

[MAKD+17] S. Matetic, M. Ahmed, K. Kostiainen, A. Dhar, D. Sommer, A. Gervais, A. Juels, and S. Capkun. ROTE: Rollback Protection for Trusted Execution. USENIX Security, 2017.

[ZEEJ+17] F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. van Renesse. REM: Resource-Efficient Mining for Blockchains. USENIX Security, 2017.

[TZLH+17]. F. Tramèr, F. Zhang, H. Lin, J.-P. Hubaux, A. Juels, and E. Shi. Sealed-Glass Proofs: Using Transparent Enclaves to Prove and Sell Knowledge. IEEE European Symposium on Security and Privacy (Euro S&P), pp. 19-34, 2017.

[TAGH+17]. F. Tramèr, V. Atlidakis, R. Geambasu, D. Hsu, J.-P. Hubaux, M. Humbert, A. Juels, and H. Lin. FairTest: Discovering Unwarranted Associations in Data-Driven Applications. IEEE European Symposium on Security and Privacy (Euro S&P), pp. 401-416, 2017.

[DEJS17]. P. Daian, I. Eyal, A. Juels, and E. G. Sirer. (Short Paper) PieceWork: Generalized Outsourcing Control for Proofs of Work. BITCOIN, 2017.

[ZCCJ+16] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi. Town Crier: An Authenticated Data Feed for Smart Contracts. ACM Conference on Computer and Communication Security (ACM CCS), pp. 270–282, 2016.

[JKS16] A. Juels, A. Kosba, and E. Shi. The Ring of Gyges: Investigating the Future of Criminal Smart Contracts. ACM Conference on Computer and Communication Security (ACM CCS), pp. 283–295, 2016.

[TZJR+16] F. Tramèr, F. Zhang, A. Juels, M. Reiter, and T. Ristenpart. Stealing Machine Learning Models via Prediction APIs. USENIX Security, pp. 601–618, 2016.

[MJ16] W. Marino and A. Juels. Setting Standards for Altering and Undoing Smart Contracts. RuleML, pp. 151–166, 2016.

[CAAJ+16] R. Chatterjee. A. Athayle, D. Akawhe, A. Juels, and T. Ristenpart. pASSWORD tYPOS and How to Correct Them Securely. IEEE Symposium on Security and Privacy (SP), pp. 800–816, 2016.
▷ **Distinguished Student Paper Award**

[CDEG+16] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer. On Scaling Decentralized Blockchains. BITCOIN, 2016.

[ECSJ+15] A. Everspaugh, R. Chatterjee, S. Scott, A. Juels, and T. Ristenpart. The Pythia PRF Service. USENIX Security, pp. 547-562, 2015.

[JKTT15] A. Juels, J. Kelley, R. Tamassia, and N. Triandopoulos. Falcon Codes: Fast, Authenticated LT Codes (Or: Making Rapid Tornadoes Unstoppable). ACM Conference on Computer and Communication Security (ACM CCS), pp. 1032-1047, 2015.

[HAHF+15] Z. Huang, E. Ayday, J.-P. Hubaux, J. Fellay, and A. Juels. GenoGuard: Protecting Genomic Data Against Brute-Force Attacks. IEEE Symposium on Security and Privacy (SP), pp. 447–462, 2015.
▷ **Distinguished Student Paper Award**

[CBJR15] R. Chatterjee, J. Bonneau, A. Juels, and T. Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. IEEE Symposium on Security and Privacy (SP), pp. 481–498, 2015.

[DGGJ+15] Y. Dodis, C. Ganesh, A. Golovnev, A. Juels and T. Ristenpart, A Formal Treatment of Backdoored Pseudorandom Generators. EUROCRYPT, pp. 101–126, 2015.

[ZJRR14] Y. Zhang, A. Juels, M. Reiter, and T. Ristenpart. Cross-Tenant Side-Channel Attacks in PaaS Clouds. ACM Conference on Computer and Communication Security (ACM CCS), pp. 990–1003, 2014.

[YHOR+14] T.-F. Yen, V. Heorhiadi, A. Oprea, M. K. Reiter, and A. Juels. An Epidemiological Study of Malware Encounters in a Large Enterprise. ACM Conference on Computer and Communication Security (ACM CCS), pp. 1117–1130, 2014.

[BHJT14] K. Bowers, C. Hart, A. Juels, and N. Triandopoulos. PillarBox: Combating Next-Generation Malware with Fast Forward-Secure Logging. Research in Attacks, Intrusions and Defenses (RAID), pp. 46–67, 2014.

[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), pp. 475–490, 2014.

[JR14a] 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), pp. 199–208, 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.

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

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

[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.

[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)**

[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. G. 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. G. 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.

[JW99] A. Juels and M. Wattenberg. A Fuzzy Commitment Scheme. ACM Conference on Computer and Communications Security (ACM CCS), pp. 28–36, 1999.
▷ **NDSS Test of Time Award, 2019**

[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. G. 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.

[JP98] A. Juels and M. Peinado. Hiding Cliques for Cryptographic Security. Symposium on Discrete Algorithms (SODA), pp. 678-684, 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.

Journal Articles

[AACJ+17] J. Aikat, A. Akella, J. S. Chase, A. Juels, M. K. Reiter, T. Ristenpart, V. Sekar, M. M. Swift. Rethinking Security in the Era of Cloud Computing. IEEE Security & Privacy 15(3): 60-69 (2017).

[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.

[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.

[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].)

[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.**

[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, Novem-

ber 2006.

[JP00] A. Juels and M. Peinado. Hiding Cliques for Cryptographic Security. *Designs, Codes, and Cryptography*, 20(3):269–280, July 2000. (Conference version appeared as [JP98].)

[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.

Invited Articles

[JEN18] A Juels, I. Eyal, and O. Naor. Blockchains won't fix internet voting security—and could make it worse. *The Conversation*, 18 October 2018.

[JBE17] A Juels, I. Bentov, and I. Eyal. By concealing identities, cryptocurrencies fuel cybercrime. *The Conversation*, 25 September 2017.

[AACJ+17] J. Aikat, A. Akella, J. S. Chase, A. Juels, M. K. Reiter, T. Ristenpart, V. Sekar, and M. Swift. Rethinking Security in the Era of Cloud Computing. IEEE Security & Privacy Magazine, 15(3): 60–69, 2017.

[JE16] A. Juels and I. Eyal. Blockchains: Focusing on bitcoin misses the real revolution in digital trust. *The Conversation*, 18 July 2016.

[EJ16] D. Estrin and A. Juels. Reassembling Our Digital Selves. *Daedalus*, Journal of the American Academy of Arts & Sciences, 145(1): 4353, Winter 2016.

[HJ16] J.-P. Hubaux and A. Juels. Privacy is Dead, Long Live Privacy: Restoring Social Norms as Confidentiality Wanes. *Communications of the ACM (CACM)*, 59(6): 39-31, June 2016.

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

[J14] A. Juels. A bodyguard of lies: the use of honey objects in information security. SACMAT, pp. 1–4, 2014.

[JR14b] A. Juels and T. Ristenpart. Honey Encryption: Encryption Beyond the Brute-Force Barrier. IEEE Security & Privacy Magazine, 12(4): 59–62, 2014.

[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.

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

[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.

Selected Technical Reports

[JS04] A. Juels and M. Syzdlo. Attribute-Based Encryption: Using Identity-Based Encryption for Access Control. RSA Labs Technical Report. 2004.

[JJ99b] A. Juels and M. Jakobsson. Millimix: Mixing in Small Batches. DIMACS TR: 99-33. 1999.

Book Chapters

[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].)

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

[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.

[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

[J09] A. Juels. *Tetraktys.* Emerald Bay Books, 2009. (A thriller novel.)

Guest Editorials / Op-Eds

[JEK21] A. Juels, I. Eyal, and M. Kelkar. Miners, Front-Running-as-a-Service Is Theft. *Coindesk.* 7 April 2021.

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

[J09b] 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.

[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.

Edited Volumes

[JP13] A. Juels and B. Parno, eds. *ACM Cloud Computing Security Workshop (CCSW)*, Co-located with ACM CCS, ACM Press, 2013.

[J04f] A. Juels and C. Paar, eds., *Security and Privacy - 7th International Workshop*, Amherst, USA, June 26-28, 2011, Revised Selected Papers. Lecture Notes in Computer Science 7055, Springer, 2012. LNCS no. 7055.

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

Professional Service

Program Chair: NDSS, 2017; ACM Conference on Communications Security, Industry Track, 2005; International Financial Cryptography Conference, 2004

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

Program "Shadow" Chair (Vice Chair): NDSS, 2016

Program Co-Chair: CCSW, 2013, RFIDSec, 2011; WiSe (ACM Workshop on Wireless Security), 2006; PerSec (Workshop on Pervasive Computing and Communication Security), 2006; DIMACS Workshop on Electronic Voting, 2004

General chair: ACM Conference on Communications Security, 2006

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; Joel Reardon, ETH-Zurich, Dec. 2014; Mathias Humbert, EPFL, January 2015; Karl Wust, ETH Zurich, August 2021

Steering Committee Member: NDSS, 2018-; ACM SIGSAC, 2005–09

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

Government Service: FCC Technical Advisory Board, 2010–11

Advisory Committee Member: RSA Conference, 2008–2012

Editorial Board Member: *Handbook of Computer Networks*, 2006; *Handbook of Information Security*, 2005; *Internet Encyclopedia*, 2004

President: International Financial Cryptography Association, 2004–2005

Technical Program Committee Member: USENIX Security, 2020; IEEE S&P, 2019; IEEE S&P, 2018; USENIX Security, 2017; BITCOIN, 2017; 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 Member: Organizer, RFID Privacy Workshop at MIT '03; Publicity chair, ACM CCS, 2001

Co-Organizer: DIMACS Workshop on Secure Cloud Computing, March 2014; RFID-CUSP Workshop, 2008

Founder: RSA Conference Cryptographers' Track (CT-RSA)

Standards Working Group Participant: ANSI X9.F1 and X9.F4

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, 2013-4

University Activity: Cornell Computer Science Ph.D. Admissions Committee, 2014-5, 2015-6; Jacobs Technion-Cornell Preparatory Committee, 2014-; Jacobs Ruch Grant Selection Committee, 2014-6

Patents

- M. Jakobsson and A. Juels. "Method and apparatus for storing information in a browser storage area of a client device." U.S. patent no. 11,064,054. Issued 13 July 2021.
- D.V. Bailey, J. G. Brainard, A. Juels, and B. S. Kaliksi, Jr. "Authentication methods and apparatus using key-encapsulating ciphertexts and other techniques." U.S. patent no. 10,958,632. Issued 23 March 2021.
- A. Juels. "Privacy-protecting system and method for wireless medical devices." U.S. patent no. 10,862,875. Issued 8 December 2020.
- A. Juels and F. Rahman. "Systems and methods for securing cryptocurrency purchases." U.S. patent no. 10,846,663. Issued 24 November 2020.
- N. Triandopoulos, K. Bowers, A. Juels, R. Rivest, and G. Luo. "Chaff password generation based on distribution-based modifications of base passwords." U.S. patent no. 10,735,403. Issued 4 August 2020.
- M. Jakobsson and A. Juels. "Method and apparatus for storing information in a browser storage area of a client device." U.S. patent no. 10,659,551. Issued 19 May 2020.
- M. Jakobsson and A. Juels. "Method and apparatus for storing information in a browser storage area of a client device." U.S. patent no. 10,594,823. Issued 17 March 2020.
- A. Juels. "Cryptographic device configured to transmit messages over an auxiliary channel embedded in passcodes." U.S. patent no. 10,367,642. Issued 30 July 2019.
- A. Juels. "Privacy-protecting system and method for wireless medical devices." U.S. patent no. 10,230,699. Issued 12 March 2019.
- A. Juels, N. Triandopoulos, and K. Bowers. "Security alerting system with dynamic buffer size adaption." U.S. patent no. 10,129,027. Issued 13 November 2018.
- A. Juels, N. Triandopoulos, and K. Bowers. "Security alerting system with network blockade policy based on alert transmission activity ." U.S. patent no. 10,104,104. Issued 16 October 2018.
- A. Juels, N. Triandopoulos, and K. Bowers. "Security alerting system with dynamic buffer size adaptation ." U.S. patent no. 9,935,770. Issued 3 April 2018.
- D. V. Bailey, J. G. Brainard, A. Juels, and B. S. Kaliski, Jr. "Authentication methods and apparatus using base points on an elliptic curve and other techniques." U.S. patent no. 9,923,718. Issued 20 March 2018.
- A. Juels and D. D. Taku. "Key provisioning method and apparatus for authentication tokens." U.S. patent no. 9,917,694. Issued 13 March 2018.
- N. Triandopoulos, A. Juels, and J. Brainard. "Forward secure one-time authentication tokens with embedded time hints." U.S. patent no. 9,871,785. Issued 16 January 2018.

- N. Triandopoulos, K. Bowers, A. Juels, R. Rivest, G. Luo. "Methods and apparatus for generating chaff passwords for use in a password-hardening system." U.S. patent no. 9,843,574. Issued 12 December 2017.
- A. Oprea, T.-F. Yen, V. Heorhiadi, M. K. Reiter, and A. Juels. "Determining risk of malware infection in enterprise hosts." U.S. patent no. 9,674,210. Issued 6 June 2017.
- A. Juels and K. D. Bowers. "Authentication token with controlled release of authentication information based on client attestation." U.S. patent no. 9,659,177. Issued 23 May 2017.
- A. Juels, N. Triandopoulos, M. van Dijk, J. Brainard, and R. Rivest. "Time synchronization solutions for forward-secure one-time authentication tokens." U.S. patent no. 9,654,467. Issued 16 May 2017.
- G. Luo and A. Juels. "Remote authentication using near field communication tag." U.S. patent no. 9,571,164. Issued 14 February 2017.
- A. Juels and R. L. Rivest. "Determining authenticity based on indicators derived from information relating to historical events." U.S. patent no. 9,537,845. Issued 3 January 2017.
- K. Ackerman, M. E. van Dijk, A. Juels, and E. Shen. "Randomly skewing secret values as a countermeasure to compromise." U.S. patent no. 9,525,551. Issued 20 December 2016.
- T.-F. Yen, A. Oprea, K. Onarlioglu, T. Leetham, W. Robertson, A. Juels, and E. Kirda. "Behavioral detection of suspicious host activities in an enterprise." U.S. patent no. 9,516,039. Issued 6 December 2016.
- A. Juels and G. Richards. "Distributed password-based authentication in a public key cryptography authentication system." U.S. patent no. 9,515,996. Issued 6 December 2016.
- A. Juels, N. Triandopoulos, M. van Dijk, and R. L. Rivest. "Methods and apparatus for silent alarm channels using one-time passcode authentication tokens." U.S. patent no. 9,515,989. Issued 6 December 2016.
- N. Triandopoulos, A. Juels, R. Tamassia, and J. A. Kelley. "Methods and apparatus for generating authenticated error correcting codes." U.S. patent no. 9,496,897. Issued 15 November 2016.
- A. Juels. "Scheduling of defensive security actions in information processing systems." U.S. patent no. 9,495,668. Issued 15 November 2016.
- A. Juels, M. van Dijk, A. Oprea, and R. L. Rivest. "Scheduling of defensive security actions in information processing systems." U.S. patent no. 9,471,777. Issued 18 October 2016.
- J. G. Brainard and A. Juels. "Generating authentication codes associated with devices." U.S. patent no. 9,467,293. Issued 11 October 2016.
- N. Triandopoulos, A. Juels, R.L. Rivest, and J. G. Brainard. "Multi-server one-time passcode verification on respective high order and low order passcode portions." U.S. patent no. 9,454,654. Issued 27 September 2016.
- T.-F. Yen, A. Juels, K. Onarlioglu, and A. Oprea. "Time sanitization of network logs from a geographically distributed computer system." U.S. patent no. 9,430,501. Issued 30 August 2016.
- N. Triandopoulos, A. Juels, and J. G. Brainard. "Multi-server passcode verification for one-time authentication tokens with auxiliary channel compatibility." U.S. patent no. 9,407,631. Issued 2 August 2016.
- G. Luo, A. Juels, and Y. Qiao. "Authentication using cryptographic value derived from a shared secret of a near field communication tag." U.S. patent no. 9,379,894. Issued 28 June 2016.
- T.-F. Yen, A. Juels, A. Kuppa, K. Onarlioglu, and A. Oprea. "Anomaly sensor framework for detecting advanced persistent threat attacks." U.S. patent no. 9,378,361. Issued 28 June 2016.

- A. Juels and S. Curry. "Distributed protection of credential stores utilizing multiple keys derived from a master key." U.S. patent no. 9,374,221. Issued 21 June 2016.
- K. D. Bowers, V. P. Dudhalkar, A. Juels, R. L. Rivest, S. Saklikar, and N. Triandopoulos. "Authentication based on user-selected image overlay effects." U.S. patent no. 9,361,447. Issued 7 June 2016.
- A. Juels. "Binding a data object to a rotational hard drive." U.S. patent no. 9,330,727. Issued 3 May 2016.
- A. Juels and K. D. Bowers. "Message encryption and decryption utilizing low-entropy keys." U.S. patent no. 9,325,499. Issued 26 April 2016.
- G. Luo, A. Juels, and K. D. Bowers. "Sharing a cryptographic device by partitioning challenge-response space ." U.S. patent no. 9,323,909. Issued 26 April 2016.
- E. Stefanov, M. Van Dijk, A. Oprea, and A. Juels. "Scalable cloud file system with efficient integrity checks." U.S. patent no. 9,323,765. Issued 26 April 2016.
- A. Juels, K. D. Ray, and G. Richards. "Password hardening system using password shares distributed across multiple servers." U.S. patent no. 9,305,161. Issued 5 April 2016.
- A. Juels, N. Triandopoulos, M. van Dijk, J. G. Brainard, R. Rivest, and K. D. Bowers. "Server methods and apparatus for processing passcodes generated by configurable one-time authentication tokens ." U.S. patent no. 9,294,473. Issued 22 March 2016.
- D. V. Bailey, B. S. Kaliski, Jr., A. Juels, and Ronald. L. Rivest. "Gaming systems with authentication token support." U.S. patent no. 9,280,871. Issued 8 March 2016.
- A. Juels, N. Triandopoulos, M. van Dijk, J. G. Brainard, R. Rivest, and K. D. Bowers. "Configurable one-time authentication tokens with improved resilience to attacks." U.S. patent no. 9,270,655. Issued 23 February 2016.
- A. Oprea, K. D. Bowers, N. Triandopoulos, T.-F. Yen, and A. Juels. "Credential recovery with the assistance of trusted entities." U.S. patent no. 9,256,725. Issued 9 February 2016.
- A. Juels, S. Todd, and Y. Yee. "Service window optimized system alert engine." U.S. patent no. 9,235,971. Issued 12 January 2016.
- A. Juels, A. Oprea, M. van Dijk, and E. Stefanov. "Remote verification of file protections for cloud data storage." U.S. patent no. 9,230,114. Issued 5 January 2016.
- A. Juels. "Methods and apparatus for obscuring a valid password in a set of passwords in a password-hardening system." U.S. patent no. 9,230,092. Issued 5 January 2016.
- J. G. Brainard, N. Triandopoulos, M. van Dijk, and A. Juels. "Event-based data signing via time-based one-time authentication passcodes." U.S. patent no. 9,225,717. Issued 29 December 2015.
- A. Juels. "Device pairing using a cryptographic commitment process involving measured motion values." U.S. patent no. 9,185,100. Issued 10 November 2015.
- A. Juels, N. Triandopoulos, K. Bowers, and C. Hart. "Methods and apparatus for secure, stealthy and reliable transmission of alert messages from a security alerting system." U.S. patent no. 9,160,539. Issued 13 October 2015.
- A. Juels. "Proactivation methods and apparatus for password-hardening systems." U.S. patent no. 9,154,496. Issued 6 October 2015.
- A. Juels and G. Luo. "Decryption of a protected resource on a cryptographic device using wireless communication." U.S. patent no. 9,154,481. Issued 6 October 2015.

- A. Juels. "Challenge-response authentication of a cryptographic device." U.S. patent no. 9,154,480. Issued 6 October 2015.
- D. V. Bailey, J. G. Brainard, A. Juels, and B. S. Kaliski, Jr. "Wireless authentication methods and apparatus." U.S. patent no. 9,137,012. Issued 15 September 2015.
- A. Juels, K. D. Bowers, B. Farley, V. Varadarajan, T. Ristenpart, and M. M. Swift. 'Determining instances to maintain on at least one cloud responsive to an evaluation of performance characteristics." U.S. patent no. 9,128,739. Issued 8 September 2015.
- A. Juels, N. Triandopoulos, and M. van Dijk. "Methods and apparatus for authenticating a user using multi-server one-time passcode verification." U.S. patent no. 9,083,515. Issued 25 August 2015.
- M. van Dijk, N. Triandopoulos, A. Juels, and R. Rivest. "Forward secure pseudorandom number generation resilient to forward clock attacks." U.S. patent no. 9,083,515. Issued 14 July 2015.
- G. Luo and A. Juels. "Distributed authentication against stored user identifiers and user templates via pseudonym association." U.S. patent no. 9,043,890. Issued May 26, 2015.
- A. Juels, S. Carielli, K. D. Bowers and G. Luo. "Distributed cryptography using distinct value sets each comprising at least one obscured secret value." U.S. patent no. 9,037,858. Issued 19 May 2015.
- A. Juels. "Self-refreshing distributed cryptography." U.S. patent 9,032,212. Issued 12 May 2015.
- T. S. Corn, A. Juels, and N. Triandopoulos."Methods and apparatus for fraud detection and remediation in knowledge-based authentication." U.S. patent 9,021,553. Issued 28 April 2015.
- A. Juels, G. Luo, and K. D. Bowers. "Cryptographic device operable in a challenge-response mode." U.S. patent 9,015,476. Issued 21 April 2015.
- T. S. Corn, A. Juels, and N. Triandopoulos. "Methods and apparatus for knowledge-based authentication using historically-aware questionnaires." U.S. patent 9,009,844. Issued 14 April 2015.
- A. Juels, A. Oprea, M. K. Reiter, and Y. Zhang. "Co-residency detection in a cloud-based system." U.S. patent 9,009,385. Issued 14 April 2015.
- A. Juels, N. Triandopoulos, and K. D. Bowers. "Method and apparatus for generating forward secure pseudorandom numbers." U.S. patent 9,008,303. Issued 14 April 2015.
- A. Juels, S. Capkun, and D. Zanetti. "Event indicator creation using first and second sets of values." U.S. patent 8,994,514. Issued 31 March 2015.
- A. Juels, N. Triandopoulos, R. L. Rivest, and M. E. van Dijk. "Methods and apparatus for embedding auxiliary information in one-time passcodes." U.S. patent 8,984,609. Issued 17 March 2015.
- A. Juels, K. D. Bowers, and A. Oprea. "Distributed storage system with efficient handling of file updates." U.S. patent 8,984,384. Issued 17 March 2015.
- A. Juels, B. S. Kaliski, K. D. Bowers, and A. Oprea. "Proof of retrievability for archived files." U.S. patent 8,984,363. Issued 17 March 2015.
- A. Juels. "Distributed challenge-response authentication." U.S. patent 8,977,847. Issued 10 March 2015.
- A. Juels and N. Triandopoulos. "Generation of exfiltration-resilient cryptographic keys." U.S. patent 8,954,728. Issued 10 February 2015.
- A. Juels and C. V. Hart. "Detection of tampering with software installed on a processing device." U.S. patent 8,938,805. Issued 20 January 2015.

- A. Juels. "Providing enhanced security for wireless telecommunications devices." U.S. patent 8,934,940. Issued 13 January 2015.
- B. M. Jakobsson and A. Juels. "Method and apparatus for storing information in a browser storage area of a client device." U.S. patent 8,930,549. Issued 6 January 2015.
- A. Juels, F. Koushanfar, and M. Rostami. "Authentication of external devices to implantable medical devices using biometric measurements." U.S. patent 8,886,316. Issued 11 November 2014.
- A. Juels and K.D. Bowers."View computation and transmission for a set of keys refreshed over multiple epochs in a cryptographic device." U.S. patent 8,874,904. Issued 28 October 2014.
- A. Juels." Conditional integration of a satellite device into an authentication process involving a primary device." U.S. patent 8,817,988. Issued 30 September 2014.
- R. Stockton, R.D. Hopley, M. van Dijk, A. Juels, and N. Triandopoulos. "Variable epoch scheduler for proactive cryptography systems." U.S. patent 8,817,988. Issued 26 August 2014.
- K. D. Bowers, M. E. van Dijk, A. Juels, A. M. Oprea, R. L. Rivest, and N. Triandopoulos. "Graph-based approach to deterring persistent security threats." U.S. patent 8,813,234. Issued 19 August 2014.
- E. P. Stefanov, M. van Dijk, A. Oprea, and A. Juels. "Remote verification of file protections for cloud data storage." U.S. patent 8,799,334. Issued 5 August 2014.
- A. Juels. "Providing enhanced security for wireless telecommunications devices." U.S. patent 8,792,862. Issued 29 July 2014.
- A. Juels and N. Triandopoulos. "Methods and apparatus for secure and reliable transmission of messages over a silent alarm channel." U.S. patent 8,788,817. Issued 22 July 2014.
- A. Juels and N. Mehta. "Apparatus and method for multi-plane threshold security." U.S. patent 8,782,752. Issued 18 July 2014.
- A. Juels. "Secret sharing in cryptographic devices via controlled release of plaintext information." U.S. patent 8,774,410. Issued 8 July 2014.
- E. P. 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. G. 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. G. 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. G. 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.

Selected Press Coverage

- *CoinDesk*. "Witnesses Debate Crypto Mining's Efficiency in Congressional Hearing on Environment," by Aoyon Ashraf and Eliza Gkritsi. 20 January 2022. (Article discussing my Congressional testimony on Bitcoin energy consumption.)

- *CoinDesk*. "Witnesses Debate Crypto Mining's Efficiency in Congressional Hearing on Environment," by Ari Juels, Ittay Eyal, and Mahimna Kelkar. 7 April 2021. (Op-ed on front-running in blockchains.)
- *Popular Science*. "A beginners guide to how cryptocurrencies work From Bitcoin to blockchain, here's what to know.," by Charlotte Hu. 15 November 2021.
- *Barron's*. "Inside DeFi, the Wild West of Cryptocurrency," by Daren Fonda. 31 October 2021.
- *Bloomberg*. "Crypto Trading: How Flashbots Work to Front-Run Ether and Other Coin Purchases," by Olga Khalif. 21 Sept. 2021.
- *The New Yorker*. "Why Bitcoin Is Bad for the Environment," by Elizabeth Kolbert. 22 April 2021.
- *Coindesk*. "Op-Ed: Miners, Front-Running-as-a-Service Is Theft," by Ari Juels, Ittay Eyal, and Mahimna Kelkar. 7 April 2021. (Op-ed on front-running in blockchains.)
- *Wired*. "As Digital Currencys Popularity Rises, So Do Privacy Fears," by Gregory Barber. 16 March 2021. (Article referencing IC3 paper on CBDC.)
- *Forbes*. "Chainlinks New Acquisition From Cornell University Could Transform Blockchain For Good," by Ben Jessel. 29 August 2020. (Article on acquisition of DECO by Chainlink.)
- *Yahoo Finance / Decrypt*. "Chainlink CEO: How 'Mixicles' can change the game for smart contract privacy," by Adriana Hamacher. 12 September 12 2019.
- *Wired*. "Microsoft Wants to Protect Your Identity With Bitcoin," by Gregory Barber. 14 May 2019. (Article on self-sovereign identity management, with references to my group's work on CHURP and oracles.)
- *Bloomberg*. "Flash Boys: Trading Bots Are Running Wild on Crypto Exchanges," by Olga Kharif and Vildana Hajric. 23 April 2019. (Article on research on cryptocurrency exchanges and arbitrage bots.)
- *MIT Tech Review China*. "The whereabouts of 4 million bitcoins worldwide are unknown? This group of Cornell University scholars want to solve this problem — Exclusive interview." 30 March 2019. (Article on secret sharing scheme robust to "churn," i.e., nodes coming and going.)
- *MIT Technology Review*. "Blockchain smart contracts are finally good for something in the real world," by Mike Orcutt. 19 November 2018. (Article on Chainlink that quotes me and discusses Town Crier.)
- *Forbes*. "Cornell's Town Crier Acquired By Chainlink To Expand Decentralized Oracle Network," by Darryn Pollock. 1 November 2018. (Article about transfer of Town Crier to Chainlink.)
- *MIT Technology Review*. "Blockchain smart contracts are finally good for something in the real world," by Mike Orcutt. 19 November 2018. (Article on Chainlink that quotes me and discusses Town Crier.)
- *Wired*. "Meet the man with a radical plan for blockchain voting," by Andrew Leonard. 16 August 2018. (Article on blockchain voting that mentions my work on vote-buying.)
- *CoinDesk*. "The 'Dark DAO' Threat: Vote Vulnerability Could Undermine Crypto Elections," by Rachel Rose O'Leary. 20 July 2018. (Article discussing my group's blog post on attacking blockchain voting systems.)
- *MIT Technology Review*. "Meet Oasis Labs, the blockchain startup Silicon Valley is buzzing about," by Mike Orcutt. 12 July 2018. (Article that discusses my group's Ekiden project and its use by Oasis Labs.)

- *CoinDesk*. "Sharding Is Ushering in Radical Ethereum Designs," by Rachel Rose O'Leary. 28 March 2018. (Article discussing GasToken / Project Chicago.)
- *CNBC*. "Bitcoin and blockchain consume an exorbitant amount of energy. These engineers are trying to change that," by Helen Zhao. 23 February 2018. (Article mentioning REM / Proof of Useful work.)
- *Bitcoin Magazine*. "Cornell IC3 Researchers Propose Solution to Bitcoins Multisig 'Paralysis' Problem," by Amy Castor. 19 January 2018. (Article on key-management research project.)
- *Gadgets 360*, "Bitcoin May Not Be the Future, but the Technology Behind It Might Well Be," by Gopal Sathe. 19 December 2017. (Interview with me regarding Bitcoin.)
- *CoinDesk*. "Smarter Bug Bounties? Hydra Codes Creative Solution for Ethereum Theft," by Rachel Rose O'Leary. 2 November 2017. (Article on Hydra Project.)
- *CoinDesk*. "Submarine Sends: IC3's Plan to Clamp Down on ICO Cheats," by Bailey Reutzel. 28 August 2017. (Article on blockchain confidentiality research.)
- *Forbes*. "Researchers Find Issues With 0x, An Ethereum-Based Project Aiming To Raise Millions In An ICO," by Amy Castor. 15 August 2017. (Article on cryptocurrency exchange research.)
- *MIT Technology Review*. "How Encrypted Weather Data Could Help Corporate Blockchain Dreams Come True," by Tom Simonite. 11 March 2017. (Article on Town Crier oracle.)
- *Wired*, "How to Steal an AI," by Andy Greenberg. 30 September 2016. (Discussion of research on "model extraction" attacks against ML model.)
- *Hacker News*, "Stealing Machine Learning Models via Prediction APIs." 22 September 2016. (Discussion of research on "model extraction" attacks against ML model.)
- *MIT Technology Review*, "Why Autocorrect for Passwords Is a Great Idea," by Tom Simonite, 1 June 2016. (Coverage of research on password-typo correction.)
- *MIT Technology Review*, "Technical Roadblock Might Shatter Bitcoin Dreams," by Tom Simonite, 16 February 2016. (Coverage of research on Bitcoin scaling.)
- *Nature*, "The Future of Cryptocurrencies: Bitcoin and Beyond," by Andy Extance, v. 526, num. 7571, 30 September 2015. (News feature covering my research on cryptocurrencies and of IC3, a research initiative that I co-direct.)
- *Phys.org*, "The Future of Encryption," by Amina Khan. 23 October 2015. (Survey of promising new encryption techniques includes honey encryption.)
- *MIT Technology Review*, "Bitcoin's Dark Side Could Get Darker," by Tom Simonite, 13 August 2015. (Coverage of research on criminal smart contracts.)
- *Slashdot*, "The Best Way To Protect Real Passwords: Create Fake Ones," 12 May 2015. (Coverage of "NoCrack" project.)
- *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.)
- *MIT Technology Review*, "Spotting Virtual Intruders," by Erica Naone, 9 March 2011. (Article on joint RSA Labs / Univ. of North Carolina work on side-channel based detection of unwanted cloud co-residency.)
- *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.)

Recent and Selected Talks

- Real World Crypto (RWC). "CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability." Jan. 2021.
- Securities and Exchange Commission (SEC), invited talk on smart contracts, Oct. 2020.
- Stanford Blockchain Conference. "Mixicles." Invited talk, Feb. 2020.
- Fireside chat with Sergey Nazarov, Chainlink CEO (in consulting capacity). Feb. 2020.
- Real World Crypto. "DECO: A privacy-preserving oracle for TLS." Invited talk, Jan. 2020.
- UPenn. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges." Distinguished Lecture. Nov. 2019.
- Cryptoeconomic Systems Summit, MIT Media Lab. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges." Invited talk. Oct. 2019.
- IC Research Day, EPFL. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges." Invited talk. June 2019.
- Cornell Blockchain Conference. "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges." Apr. 2019.
- New York Family Office and High Net Worth Blockchain Conference. "Intro to Smart Contracts." Invited talk. Nov. 2018.
- Hasso-Plattner-Institut für Digital Engineering, NYC, HPI Cybersecurity Symposium. "Intro to Smart Contracts." Invited talk. Sept. 2018.
- TU Darmstadt, "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts." Distinguished Lecture Series talk. June 2018.
- Summer Research Institute (SuRI), EPFL. "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts." Invited talk. June 2018.
- Summer School on Real-World Crypto and Privacy, Sibenik, Croatia. "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts." Invited talk. June 2018.

- MIT Bitcoin Expo, "Trusted-Hardware and Blockchain Alchemy: Oracles, Paralysis Proofs, Exchanges, and More." Invited talk. March 2018.
- George Mason University, "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts." Distinguished Lecture Series talk. March 2018.
- Cambridge Blockchain Meetup, "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts." March 2018.
- Networks and Distributed Security Systems (NDSS), "Beyond Smarts: Toward Correct, Private, Data-Rich Smart Contracts." Keynote talk. February 2018.
- Information Theory and Applications Workshop, "Beyond Smarts: Toward Correct, Private, Data-Rich Smart Contracts." Plenary session talk. February 2018.
- UC Berkeley, "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts." Bay Area Crypto Day. November 2017.
- UCSD, "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts." Distinguished Lecture Series talk. November 2017.
- Summer School on Real-World Crypto and Privacy, Sibenik, Croatia. "Blockchains and Trusted Hardware." Invited talk. June 2017.
- Summer Research Institute (SuRI), EPFL. "Solidus: Strong Confidentiality and Transparency for Blockchain Transactions." Invited talk. June 2017.
- NYC IC3 Meetup, "Town Crier: An Authenticated Data Feed for Smart Contracts." September 2016.
- Cx / AOL-Cornell Tech workshop, NYC, "The Jekyll and Hyde of Smart Contracts." Keynote talk. August 2016.
- Summer Research Institute (SuRI), EPFL. "Exploring the Future of Smart Contracts." Invited talk. June 2016.
- NYU, "The Ring of Gyges: Exploring the Future of Criminal Smart Contracts." Invited talk. April 2016.
- NSF WATCH series, "The Jekyll and Hyde of Smart Contracts." April 2016.
- Institute of International Finance (IIF), Invited Tutorial on Smart Contracts. April 2016.
- MIT, "The Ring of Gyges: Exploring the Future of Criminal Smart Contracts." Invited talk. April 2016.
- Real World Cryptography, Stanford University "PASS: Strengthening and Democratizing Enterprise Password Hardening." Invited talk. January 2016.
- Army Research Office cyberdeception workshop, George Mason University "A Bodyguard of Lies: The Use of Honey Objects in Information Security." Invited talk. August 2015.
- Summer Research Institute (SuRI), EPFL. "The Ring of Gyges: Using Smart Contracts for Crime." Invited talk. June 2015.
- The Technion. "The Ring of Gyges: Using Smart Contracts for Crime." May 2015.
- Google Faculty Research Summit, Mountain View, CA, USA. "Parallax Privacy." March 2015.
- Qualcomm Research, Santa Clara, CA, USA. "A Bodyguard of Lies: The Use of Honey Objects in Information Security." March 2015.
- ACM SACMAT, Waterloo, Canada. "A Bodyguard of Lies: The Use of Honey Objects in Information Security." Keynote talk. June 2014.

- Summer Research Institute (SuRI), EPFL. "The Password That Never Was." June 2014.
- ETH-Zurich. "The Password That Never Was." Distinguished Colloquium. March 2014.
- Harvard University "The Password That Never Was." March 2014.
- University of Waterloo. "The Password That Never Was." February 2014.
- Carnegie Mellon University "The Password That Never Was." January 2014.
- Johns Hopkins University "The Password That Never Was." October 2013.
- Google-UMD Cybersecurity Seminar Series, UMD. "Aggregation and Distribution in Cloud Security." Invited talk. March 2013.
- Boston University "Aggregation and Distribution in Cloud Security." March 2013.
- University of Washington. "Aggregation and Distribution in Cloud Security." February 2013.
- RSA Conference Cryptographers' Panel (Keynote), San Francisco, CA, USA. Moderator. February 2013.
- Real World Cryptography, Stanford University "The Challenges of Distributing Distributed Cryptography." Invited talk. January 2013.
- MIT Security Seminar. "Breaks in the Cloud." November 2012.
- SecureCloud, Frankfurt, Germany. "Aggregation and Distribution in Cloud Security." Invited talk. May 2012.
- RSA Conference Cryptographers' Panel (Keynote), San Francisco, CA, USA. Moderator. March 2012.
- Schloss Dagstuhl joint seminar on cloud security, Dagstuhl, Germany. "Crypto in the Cloud or *Ignis Fatuus* in the Swamp?" Keynote talk. December 2011.
- UW MSR Summer Institute, Cle Elum, WA, USA. "Crypto for the Cloud: From the Mythological to the Merely Impossible-Seeming. July 2011.
- RSA Conference Cryptographers' Panel (Keynote), San Francico, CA, USA. Moderator. March 2011.
- Workshop on Cryptography and Security in Clouds, ETH-Zurich. "Writing on Wind and Water: Storage Security in the Cloud." Invited talk. March 2011.
- Microsoft Research, Redmond, WA, USA. "Writing on Wind and Water: Enforcing File Robustness in the Cloud." August 2010.
- Summer Research Institute (SuRI), EPFL . "Writing on Wind and Water: Enforcing File Robustness in the Cloud." Invited talk. June 2010.
- RFIDSec, Istanbul, Turkey. "The Physical Basis of RFID Security." Keynote talk. June 2010.
- RSA Conference Cryptographers' Panel (Keynote), San Francisco, CA, USA. Moderator. March 2010.
- Authors@Google, "Tetraktys." San Francisco, CA, USA. March 2010.
- International Workshop on RFID Security and Cryptography (RISC), London, U.K. "Power Games in RFID Security." Keynote talk. November 2009.
- U.C. Berkeley. "Proofs of Retrievability: Toward RAID in the Cloud." October 2009.
- RSA Conference Cryptographers' Panel (Keynote), San Francisco, CA, USA. Moderator. April 2009.

- FTC Workshop on Contactless Payment Technology, Washington, D.C., USA. Panelist. October 2008.
- WiSec, Alexandria, VA, USA. "RFID in the Shoulder and on the Loading Lock." Keynote talk. March 2008.
- Conference on Hardware and Embedded System Security (CHES), Yokohama, Japan. "The Outer Limits of RFID Security." Invited talk. October 2006.
- USENIX Security, San Diego, CA, USA. "RFID: Privacy and Security for Five-Cent Computers." Invited talk. August 2004.
- U.S. Federal Trade Commission RFID Workshop, Washington, D.C., USA. Panelist. June 2004.
- U.S. Senate Judiciary Committee Staff Briefing, Washington, D.C., USA. Panelist. June 2004.
- U.S. Department of Commerce Wireless Sensor Technology Forum, Washington, D.C., USA. Panelist. April 2004.
- l'Ecole Normale Supérieure. "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes" and "Nightingale: Distributed Cryptography for the Masses." May and June 2003
- M.I.T. Cryptography and Infosec Group. "Fuzzy Commitment." September 2002.
- United States Patent and Trademark Office. "Selected Topics in Cryptography." June 2001.
- United States Patent and Trademark Office. "Cryptography: An Introduction and Discussion of Recent Trends." August 1999.
- Bell Laboratories, Murray Hill, NJ, USA. "Removing Paper-and-Pencil Metaphors from Cryptography." Invited talk. June 1999.
- Carnegie Mellon University "The Equilibrium Genetic Algorithm." March 1996.