Bryan Ford

Updated February 10, 2023

EPFL – IC – DEDIS
BC 210, Station 14
CH-1015 Lausanne
Switzerland

Phone: +41 (0)21 693 28 73
E-mail: bryan.ford@epfl.ch
Web: https://bford.info/
ORCID: 0000-0002-0528-3033

Academic Positions

Associate Professor — 2015–
School of Computer and Communication Sciences — École Polytechnique Fédérale de Lausanne
Research topics: Decentralized/distributed systems, security/privacy, anonymity, anti-censorship.

Associate Professor (tenured 2014) — 2014–2015
Assistant Professor — 2009–2014
Department of Computer Science — Yale University
Research topics: Decentralized/distributed systems, security/privacy, Internet architecture.

Postdoctoral Researcher — 2008–2009
Advisor: Peter Druschel — Max Planck Institute for Software Systems
Research focus: next-generation Internet architecture.

Education

Ph.D. and M.Sc. Computer Science, Massachusetts Institute of Technology, September 2008
Ph.D. Thesis title: *UIA: A Global Connectivity Architecture for Mobile Personal Devices*
M.Sc. Thesis title: *Packrat Parsing: a Practical Linear-Time Algorithm with Backtracking*
Thesis Advisor: M. Frans Kaashoek

B.Sc. Computer Science, University of Utah, June 1998, *summa cum laude*
Thesis Advisor: Jay Lepreau

Teaching Activities

Technologies of societal self-organization (EPFL CS-234)	Fall '19–'22
Decentralized Systems Engineering (EPFL CS-438)	Fall '17–'22
CS for Lawyers and Policy Workers (EPFL Continuing Education)	Spring '18
Information Security and Privacy (EPFL COM-402)	Spring '17, '18
Principles of Computer Systems (EPFL CS-522)	Fall '15
Computer Networks (EPFL COM-208)	Fall '15
Introduction to Programming (Yale CPSC 112)	Spring '15
Operating Systems (Yale CPSC 422)	Spring '10, '11, '13, '14
Building Decentralized Systems (Yale CPSC 426)	Fall '10, '12, '13, '14
Advanced Systems Topics Seminar (Yale CPSC 722)	Fall '09, '11, '12

Invited participation in other courses

IMD TransformTech – blockchain technology module	Jan '19, Sep '19, Jan '20, Sep '20
IML Information Systems & Big Data – Digital Security	May '19, May '20

Research Supervision (selected)

PhD advisees and co-advisees (current)	*Thesis topic (tentative)*	*Period*
Enis Ceyhun Alp	Heterogeneous sharded blockchains	2017–
Simone Colombo	Verifiable private information retrieval	2019–
Haoqian Zhang	Cryptocurrencies and monetary policy	2020–
Pasindu Tennage	Performance-resilient consensus	2020–
Louis-Henri Merino	Coercion-resistant E-voting	2020–

PhD advisees (completed)	*Thesis topic*	*Completion*
Cristina Băsescu	Systems Resilient to Failures, Partitions, and Slowdowns	2022
Georgia Fragkouli	Toward Internet Performance Transparency	2022
Kirill Nikitin	Integrity and Metadata Protection in Data Retrieval	2021
Ludovic Barman	Analyzing and Protecting Communication Metadata	2021
David Froelicher	Privacy-Preserving Federated Analytics	2021
Eleftherios Kokoris-Kogias	Secure Confidential Blockchains with High Throughput and Low Latency	2019
Ewa Syta	Identity Management through Privacy-Preserving Authentication	2015
Ennan Zhai	Structural Reliability Auditing for Cloud Computing	2015
Weiyi Wu	Warding off Timing Channels in Deterland	2015
John Maheswaran	Privacy-Preserving Credentials from Federated Identities	2015
Michael F. Nowlan	Wire-Compatible TCP for Low-Latency Applications	2014
Amittai Aviram	Deterministic OpenMP	2012

PhD committees	*Institution*	*Thesis topic*	*Completion*
Aljosha Judmayer	TU Vienna	Pay to Win	2022
Lihi Idan	Yale University	Data exploitation and privacy protection	2021
Darya Melnyk	ETHZ	Byzantine Agreement on Representative Input Values	2020
Severin Hauser	U. Fribourg	Broadcast Channel With Memory and Bulletin Board	2020
Hoang-Long Nguyen	U. Lorraine	Blockchain based transparency system	2019
Zhicong Huang	EPFL	Secure Cloud Computing for Genomic Data	2018
Alevtina Dubovitskaya	EPFL	Privacy-Preserving Data Exchange and Aggregation	2018
Maxime Augier	EPFL	Trustworthy Cloud Storage	2016
Berker Ağir	EPFL	Context and semantic aware location privacy	2016
Hao Zhuang	EPFL	Multicloud Resource Allocation	2016
Arthur Gervais	ETHZ	Proof of Work Blockchains	2016
Mahdi Zamani	U. New Mexico	Scalable Anonymous Communication	2016
Iris Safaka	EPFL	Unconditional security and privacy	2016
Rafik Chaabouni	EPFL	Set Membership and Range Proofs	2016
Daniel Winograd-Cort	Yale U.	Effects, Asynchrony, and Choice in AFRP	2015
Sangman Kim	UT Austin	Networking Abstractions for GPU Programs	2015
Shu-Chun Weng	Yale U.	Modular Certified Programming	2015
Andreas Voellmy	Yale U.	Scalable SDN controllers	2014
Hongqiang Liu	Yale U.	Traffic Planning under Network Dynamics	2014
Alexander Thomson	Yale U.	Deterministic Database Systems	2013
Alexander Vaynberg	Yale U.	Certified Virtual Memory Manager	2012
Yair Sovran	New York U.	Scalable geo-replicated storage	2012
Anton Burtsev	U. Utah	Deterministic systems analysis	2012

Postdocs and Resarch Scientists	*Research topic*	*Period*
Vero Estrada-Galiñanes	Decentralized Storage Systems	2021–
David Lazar	Private and Anonymous Communication Systems	2019–2021
Henry Corrigan-Gibbs	Secure and Privacy-Preserving Information Processing	2019–2020
Eleftherios Kokoris-Kogias	Secure Scalable Decentralized Systems	2019–2020
Philipp Jovanovic	Scalable, Transparent Decentralized Systems	2015–2019
Stevens Le Blond	Mobile Operating System Security and Privacy	2017–2018
David Isaac Wolinsky	Disruption-Proof Anonymous Communication	2011–2015
Syed Obaid Amin	Next-generation Transport Services	2009–2012

External Research Funding

Humanitarian Action Challenges (HAC) grant *PAIDIT: Private Anonymous Identity for Digital Transfers,* Bryan Ford (PI), Alexandre Gachoud, Vincent Graf Narbel, Mark Staehle. Jan 2022–Dec 2023, CHF 291,096.

EU H2020 grant 825377: *UNICORE: A Common Code Base and Toolkit for Deployment of Applications to Secure and Reliable Virtual Execution Environments*, Joel Nider (PI), Felipe Huici, Bryan Ford, Costin Raiciu, Caterina Parals, Laurent Mathy, Trevor Moore, Herbert Bos, Nicola Ciulli, Thierry Masson, Cristian Patachia-Sultanoiu, Radu Stoenescu (co-PIs). Dec 2019–Nov 2022, EUR 5,411,766.

EIT Health project: *TWINs: Secure, auditable patient consent,* Bryan Ford (PI) and Sylke Hoehnel. July 2019–Dec 2020, EUR 750,000.

ONR grant N000141912361: *Privacy-preserving foundation for online personal identity,* Bryan Ford (PI). May 2019–Apr 2022, $393,544.80.

Swiss Reinsurance Corporation: bilateral research project, Bryan Ford (PI). Jan 2019–Dec 2019, CHF 150,000.

ByzGen: bilateral research project on blockchain security, Bryan Ford (PI). Nov 2018–Oct 2019, CHF 115,000.

Geneva Canton: bilateral research project on E-voting, Bryan Ford (PI). Jul 2018–Jun 2019, CHF 150,000.

SICPA: bilateral research project on digital document security. Bryan Ford (PI). Jan 2018–Mar 2018, CHF 23,200.

Swiss Data Science Center (SDSC) project: *Security and Privacy of the Data Science Knowledge Graph,* Jean-Pierre Hubaux (PI) and Bryan Ford (co-PI). Jan 2018–Dec 2019, CHF 577,000.

Public Health and Related Technologies (PHRT) project: *DPPH: Data Protection in Personalized Health*. Jean-Pierre Hubaux (PI), Bryan Ford, Dimitar Jetchev, Jacques Fellay, Effy Vayena, and Olivier Verscheure (co-PIs). Jan 2018–Dec 2020, CHF 2,984,500.

DHS grant FA8750-16-2-0034: *PriFi Networking for Tracking Resistant Mobile Computing,* Joan Feigenbaum (PI), David Isaac Wolinsky, and Bryan Ford (co-PIs). Feb 2016–Jan 2019, $1,727,334.

AXA Research Program: *Privacy-Preserving Decentralized Systems and Emergent Risks from Big Data Computing,* Bryan Ford (PI). Sep 2015–2025, CHF 1,500,000.

NSF TWC-1409599: *Hiding Hay in a Haystack: Integrating Censorship Resistance into the Mainstream Internet,* Vitaly Shmatikov (PI) and Bryan Ford (co-PI). Sep 2014–Aug 2018, $600,000.

NSF CNS-1407454: *An App-Centric Transport Architecture for the Internet,* Hari Balakrishnan (PI) and Bryan Ford (co-PI). Sep 2014–Aug 2018, $399,999.

Cisco University Research Grant, *The Minion Suite: A Network-Compatible Datagram Substrate for Internet Applications and Transports,* Janardhan Iyengar (PI) and Bryan Ford. Sep 2012, $98,999.

NSF CNS-1149936: *CAREER: From Storm Clouds to EverCouds: Heading Off Long-Term Cloud Computing Risks,* Bryan Ford (PI). Jun 2012–May 2016, $450,000.

ONR grant N000141210478: *Reasoning Infrastructure for Security-Aware Software Development,* Bryan Ford (PI), Joan Feigenbaum, and Zhong Shao. Apr 2012–Mar 2015, $750,000.

NSF CNS-1065451: *Making OS Kernels Crash-Proof by Design and Certification,* Zhong Shao (PI) and Bryan Ford. Aug 2011–Jul 2015, $1,116,262.

DARPA SAFER contract N66001-11-C-4018: *Dissent: Scalable and Disruption-Proof Anonymity for Interactive Internet Communication,* Bryan Ford (PI), Joan Feigenbaum, and Vitaly Shmatikov. Dec 2010–Oct 2014, $3,699,999.

DARPA CRASH award FA8750-10-2-0254: *Advanced Development of Certified OS Kernels,* Zhong Shao (PI) and Bryan Ford. Oct 2010–Sep 2014, $2,657,704.

NSF CNS-1017206: *An Operating System and Programming Model for Deterministic Parallel Computation,* Bryan Ford (PI). Aug 2010–Jul 2013, $472,130.

ONR grant N00014-09-10757: *Proactively Removing the Botnet Threat,* Joan Feigenbaum (PI), Steven M. Bellovin, Angelos Keromytis Salvatore J. Stolfo, Vitaly Shmatikov, Michael Walfish, and Bryan Ford. Apr 2009–Sep 2010, $883,627.

NSF CNS-0916413: *Tng, a Next Generation Transport Services Architecture,* Bryan Ford (PI) and Janardhan Iyengar. Aug 2009–Jul 2011, $328,260.

Outreach Activities

Broader-audience and popular media writing (selected)		*Year*
Technologizing Democracy or Democratizing Technology?	Digital Technology & Democratic Theory	2020
The Remote Voting Minefield	personal web site	2019
Apple, FBI, and Software Transparency	Freedom to Tinker	2016
Seeking Anonymity in an Internet Panopticon	Communications of the ACM	2015
GPUfs: the case for operating system services on GPUs	Communications of the ACM	2014
Technology Can Make Lawful Surveillance Open and Effective	MIT Technology Review	2014
Is Data Hoarding Necessary for Lawful Surveillance?	Huffington Post	2014
Delegative Democracy (early formulation of liquid democracy)	personal web site	2002

Technology standardization activities	*Year*
IETF and IRTF security and cryptography working groups	2015–
IETF transport and NAT working groups (co-authored 4 RFCs)	2005–2010

Work drawing popular media coverage	*Year*	
Riffle anonymity system	20+ articles in multiple languages	2016
Apple, FBI, and Software Transparency blog post	10+ articles and radio interviews	2016
Open letter opposing mass surveillance	4+ articles	2014
Dissent anonymity system	5+ articles	2013–2016
Icebergs in the Clouds workshop paper	15+ articles in multiple languages	2010
Deterministic timing channel control paper	1 article	2010

Technology advising and consulting (selected)		*Year*
Taurus Group	Blockchain technology	2018–
Chainspace	Blockchain technology	2018–2019
Richemont	Blockchain technology	2018
ByzGen	Blockchain technology	2017–2019
DFINITY	Consensus and blockchain technology	2017–2019
Swisscom Digital Lab	Blockchain technology	2017
International Committee of the Red Cross	Digital trust and data protection	2016–
SICPA	Cryptocurrencies and blockchain technology	2015

Scientific Service Activities

Conference and workshop program committees	*Year*
OSDI, NSDI, IEEE S&P, E-Vote-ID	2023
EuroSys, PETS	2022
CCS, EdgeSys, AFT	2021
EuroSys	2020
NSDI, FC, AFT, Tokenomics	2019
FC, BPASE, CVCBT	2018
PETS, ASPLOS ERC, BITCOIN, IEEE S&B	2017
OSDI, PLDI, PETS, WWW	2016
SOSP, IEEE S&P, SIGCOMM, SAT, RAID	2015
OSDI, EuroSys, APSys, FOCI	2014
SOSP, ASPLOS, NSDI, WWW, SYSTOR	2013
EuroSys, CCS, ASPLOS ERC, WoDet, CCSW	2012
SOSP, USENIX, CCS, CCSW, MobiHeld	2011
OSDI, HotNets	2010
IMC, NPSec, ICCCN	2009
ROADS	2008

Scientific event organization	*Year*
JEDI Billion Molecules against Covid-19 grand challenge: scientific committee	2020
Swiss Blockchain Winter School	2019
USENIX ATC: program chair	2017
DARPA ISAT: Technologies for Scalable Self-Organizing Communities: organizer	2017
Swiss Blockchain Summer School	2017
Hot Topics in Networking (HotNets) workshop: program chair	2016
DARPA ISAT: Technological Disruptions of Societies and Organizations: organizer	2016
DARPA ISAT: The EverCloud: Anticipating and Countering Cloud-Rot: organizer	2014
Workshop on Determinism (WoDet): program chair	2011
SOSP Poster/WIP session: program chair	2011
PFLDnet: program chair	2010

Other scientific service	*Year*
US National Science Foundation (NSF) review panelist	2010, 2011, 2013, 2014
DARPA Information Science and Technology (ISAT)	2014–2017

Advisory board memberships	*Year*
Tribu Foundation	2018–2019
Swiss Fintech Innovations (SFTI)	2017–

Invited lectures and consultations (selected)	*Year*
Swiss Federal Chancellery – independent examination of the Swiss Post e-voting system	2021–2022
Swiss Federal Chancellery – consultation on redesign of Internet voting trials in Switzerland	2020
AXA Days keynote on digital trends, risks, and opportunities	2020
ETHZ Distinguished Computer Science Colloquium: Que Sera Consensus	Nov 2019
Wilton Park conference: Digital Dignity in armed conflict	Oct 2019
International Summer School on Security & Privacy for Blockchains: Coins, Clubs, and Crowds	Sep 2019
World Conference of Science Journalists: panel Blockchain: a silent revolution?	Jul 2019
Geneva Grand Council commission on political rights – blockchain and E-voting	Mar 2019
American Institute of Architects (AIA) Committee on Design (COD): Participatory Democracy	Sep 2019
Swiss Symposium on Blockchain Research: Decentralized Data Protection	May 2019
JPEG Workshop on Media Blockchain: Blockchain and Data Protection	Mar 2019
International Committee of the Red Cross (ICRC) – blockchain and digital identity	Feb 2019
Computers, Privacy & Data Protection (CPDP): Decentralized Identity	Feb 2019
Keynote: Second Annual Delft Blockchain Symposium	Jan 2019
Keynotes at Democracia 2050 and Congresu Futuro, Chile – liquid democracy	Jan 2018
AXA IoT & Data Protection – Blockchain and IoT	Oct 2017
Swiss Cyber Storm – E-voting security	Oct 2017
Swiss Federal Chancellery E-voting council: Blockchain and E-voting	Sep 2017
50 Years of the ACM Turing Award Celebration – Privacy and National Security	Jun 2017
Swiss Academy of Engineering Sciences (SATW) – Blockchain technology	May 2017
International School on Foundations of Security Analysis and Design (FOSAD)	2016
Keynote at ACM International Systems and Storage Conference (SYSTOR)	2016
Keynote at Workshop on Foundations of Computer Security (FCS)	2016
Keynote at Italian AXA Forum	2016
Keynote at ICISSP conference – Grand Challenges in Internet Anonymity	2015
Dissent project: invited talks at 10+ research institutions	2011–2015
Privacy vs. Security policy panelst at George C. Marshall Institute, Washington, D.C.	2014
Keynote at NDSS SENT workshop	2014

Awards and Distinguished Memberships (selected)

ACM CCS Test-of-Time Award for "Dissent: Accountable Anonymous Group Messaging"	2020
IRTF Applied Networking Research Prize (ANRP) for "MorphIT"	2020
BILANZ and Le Temps – Digital Shapers 2019	2019
IEEE Security & Privacy Distinguished Paper Award for "Digital Immunity"	2018
Initiative for CryptoCurrencies & Contracts (IC3) Member	2017–
Swiss Fintech Innovations (SFTI) Advisory Board Member	2017–
AXA Research Fund Chair in Information Security and Privacy	2015
DARPA Information Science and Technology (ISAT) Advisory Group	2014–2017
NSF Faculty Early Career Development (CAREER) Award	2012
Jay Lepreau Best Paper award for "Efficient System-Enforced Deterministic Parallelism"	2010
Best Student Paper award for "Vx32: Lightweight User-level Sandboxing on the x86"	2008
Presidential Fellowship, Massachusetts Institute of Technology	2000
Inaugural Computing Research Association Outstanding Undergraduate Award	1995
Barry M. Goldwater Excellence in Education scholarship	1994
Clyde Christensen College of Engineering scholarship, Univeristy of Utah	1991

Refereed Journal Publications

1. *Moby: A Blackout-resistant Anonymity Network for Mobile Devices*, Amogh Pradeep, Hira Javaid, Antoine Rault, David Choffnes, Stevens Le Blond, and Bryan Ford. *Proceedings of Privacy Enhancing Technologies (PoPETS)* 2022(3).
2. *PriFi: Low-Latency Anonymity for Organizational Networks*, Ludovic Barman, Italo Dacosta, Mahdi Zamani, Ennan Zhai, Apostolos Pyrgelis, Bryan Ford, Jean-Pierre Hubaux, and Joan Feigenbaum. *Proceedings of Privacy Enhancing Technologies (PoPETS)* 2020(4).

3. *Reducing Metadata Leakage from Encrypted Files and Communication with PURBs*, Kirill Nikitin, Ludovic Barman, Wouter Lueks, Matthew Underwood, Jean-Pierre Hubaux, and Bryan Ford. *Proceedings of Privacy Enhancing Technologies (PoPETS)* 2019(4), October 2019.
4. *MorphIT: Morphing Packet Reports for Internet Transparency*, Georgia Fragkouli, Katerina Argyraki, and Bryan Ford. **Winner of IRTF Applied Networking Research Prize (ANRP).** *Proceedings of Privacy Enhancing Technologies (PoPETS)* 2019(2), May 2019.
5. *MedCo: Enabling Secure and Privacy-Conscious Exploration of Distributed Clinical and Genomic Data*, Jean Louis Raisaro, Juan Ramón Troncoso-Pastoriza, Mickaël Misbach, João Sá Sousa, Sylvain Pradervand, Edoardo Missiaglia, Olivier Michielin, Bryan Ford, and Jean-Pierre Hubaux. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, July 2018.
6. *UnLynx: A Decentralized System for Privacy-Conscious Data Sharing*, David Froelicher, Patricia Egger, João Sá Sousa, Jean Louis Raisaro, Zhicong Huang, Christian Mouchet, Bryan Ford, and Jean-Pierre Hubaux. *Proceedings of Privacy Enhancing Technologies* 2017 (4), October 2017.
7. *Riffle: An Efficient Communication System With Strong Anonymity*, Albert Kwon, David Lazar, Srinivas Devadas, and Bryan Ford. *Proceedings of Privacy Enhancing Technologies (PoPETS)* 2016(2), December 2015.
8. *Security Analysis of Accountable Anonymity in Dissent*, Ewa Syta, Aaron Johnson, Henry Corrigan-Gibbs, Shu-Chun Weng, David Wolinsky, and Bryan Ford. *ACM Transactions on Information and System Security (TISSEC)* 17(1), August 2014.
9. *GPUfs: Integrating a File System with GPUs*, Mark Silberstein, Bryan Ford, Idit Keidar, and Emmett Witchel. *ACM Transactions on Computing Systems (TOCS)* 32(1), February 2014.
10. *A Dynamic Recursive Unified Internet Design (DRUID)*, J. Touch, I. Baldine, R. Dutta, G. Finn, B. Ford, S. Jordan, D. Massey, A. Matta, C. Papadopoulos, P. Reiher, and G. Rouskas. Computer Networks 55(4), March 2011.

Book Chapters

11. *Technologizing Democracy or Democratizing Technology? A Layered-Architecture Perspective on Potentials and Challenges*, Bryan Ford. In *Digital Technology and Democratic Theory* by Lucy Bernholz, Hélène Landemore, and Rob Reich (editors), The University of Chicago Press, May 2020.

Refereed Conference Publications

1. *Authenticated Private Information Retrieval*, Simone Colombo, Kirill Nikitin, Bryan Ford, David J. Wu, and Henry Corrigan-Gibbs, USENIX Security Symposium, August 2023.
2. *CALYPSO: Private Data Management for Decentralized Ledgers*, Eleftherios Kokoris-Kogias, Enis Ceyhun Alp, Linus Gasser, Philipp Jovanovic, Ewa Syta, and Bryan Ford. 47th International Conference on Very Large Data Bases (VLDB), August 16–20, 2021.
3. *On the Security of Two-Round Multi-Signatures*, Manu Drijvers, Kasra Edalatnejad, Bryan Ford, Eike Kiltz, Julian Loss, Gregory Neven, and Igors Stepanovs. IEEE Security & Privacy, May 2019.
4. *OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding*, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ewa Syta, and Bryan Ford. IEEE Security & Privacy, May 2018.
5. *On Enforcing the Digital Immunity of a Large Humanitarian Organization*, Stevens Le Blond, Alejandro Cuevas, Juan Ramón Troncoso-Pastoriza, Philipp Jovanovic Bryan Ford, and Jean-Pierre Hubaux. **Winner of Distinguished Paper Award.** IEEE Security & Privacy, May 2018.
6. *Atom: Horizontally Scaling Strong Anonymity*, Albert Kwon, Henry Corrigan-Gibbs, Srinivas Devadas, and Bryan Ford. ACM Symposium on Operating Systems Principles (SOSP), October 2017.
7. *CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds*, Kirill Nikitin, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Justin Cappos, and Bryan Ford. USENIX Security Symposium, August 2017.

8. *Scalable Bias-Resistant Distributed Randomness*, Ewa Syta, Philipp Jovanovic, Eleftherios Kokoris Kogias, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Michael J. Fischer, and Bryan Ford. IEEE Security & Privacy, May 2017.
9. *Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing*, Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. USENIX Security Symposium, August 2016.
10. *Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning*, Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford. IEEE Security & Privacy, May 2016.
11. *AnonRep: Towards Tracking-Resistant Anonymous Reputation*, Ennan Zhai, David Isaac Wolinsky, Ruichuan Chen, Ewa Syta, Chao Teng, and Bryan Ford. NSDI, March 2016.
12. *Building Privacy-Preserving Cryptographic Credentials from Federated Online Identities*, John Maheswaran, Daniel Jackowitz, Ennan Zhai, David Isaac Wolinsky, and Bryan Ford. CODASPY, March 2016.
13. *Deterministically Deterring Timing Attacks in Deterland*, Weiyi Wu and Bryan Ford. TRIOS, October 2015.
14. *Private Eyes: Secure Remote Biometric Authentication*, Ewa Syta, Michael J. Fischer, David Wolinsky, Abraham Silberschatz, Gina Gallegos-Garcia, and Bryan Ford. SECRYPT, July 2015.
15. *Heading Off Correlated Failures through Independence-as-a-Service*, Ennan Zhai, Ruichuan Chen, David Isaac Wolinsky, and Bryan Ford. OSDI, October 2014.
16. *Managing NymBoxes for Identity and Tracking Protection*, David Isaac Wolinsky, Daniel Jackowitz, and Bryan Ford. TRIOS, October 2014.
17. *TAQ: Enhancing Fairness and Performance Predictability in Small Packet Regimes*, Jay Chen, Lakshmi Subramanian, Janardhan Iyengar, and Bryan Ford. EuroSys, April 2014.
18. *Hang With Your Buddies to Resist Intersection Attacks*, David Isaac Wolinsky, Ewa Syta, and Bryan Ford. 20th ACM Conference on Computer and Communications Security, November 2013.
19. *Ensuring High-Quality Randomness in Cryptographic Key Generation*, Henry Corrigan-Gibbs, Wendy Mu, Dan Boneh, and Bryan Ford. 20th ACM Conference on Computer and Communications Security, November 2013.
20. *Proactively Accountable Anonymous Messaging in Verdict*, Henry Corrigan-Gibbs, David Isaac Wolinsky, and Bryan Ford. 22nd USENIX Security Symposium, August 2013.
21. *Maple: Simplifying SDN Programming Using Algorithmic Policies*, Andreas Voellmy, Junchang Wang, Y. Richard Yang, Bryan Ford, and Paul Hudak. ACM SIGCOMM, August 2013.
22. *GPUfs: Integrating a File System with GPUs*, Mark Silberstein, Bryan Ford, Idit Keidar, and Emmett Witchel. 18th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), March 2013.
23. *Enhancing the OS Against Security Threats in System Administration*, Nuno Santos, Rodrigo Rodrigues, and Bryan Ford. 2012 ACM/IFIP/USENIX International Middleware Conference (Middleware), December 2012.
24. *Dissent in Numbers: Making Strong Anonymity Scale*, David Isaac Wolinsky, Henry Corrigan-Gibbs, Bryan Ford, and Aaron Johnson. 10th USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 2012.
25. *Fitting Square Pegs Through Round Pipes: Unordered Delivery Wire-Compatible with TCP and TLS*, Michael Nowlan, Nabin Tiwari, Janardhan Iyengar, Syed Obaid Amin, and Bryan Ford. 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI), April 2012.
26. *Eyo: Device-Transparent Personal Storage*, Jacob Strauss, Justin Mazzola Paluska, Chris Lesniewski-Laas, Bryan Ford, Robert Morris, and Frans Kaashoek. USENIX Annual Technical Conference, June 2011.
27. *Efficient System-Enforced Deterministic Parallelism*, Amittai Aviram, Shu-Chun Weng, Sen Hu, and Bryan Ford. **Winner of Jay Lepreau Best Paper Award.** 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 2010.

28. *Dissent: Accountable Anonymous Group Messaging*, Henry Corrigan-Gibbs and Bryan Ford. **Winner of ACM CCS Test-of-Time Award.** 17th ACM Conference on Computer and Communications Security (CCS), October 2010.
29. *Vx32: Lightweight User-level Sandboxing on the x86*, Bryan Ford and Russ Cox. **Winner of Best Student Paper Award.** USENIX Annual Technical Conference (USENIX), June 2008.
30. *Alpaca: Extensible Authorization for Distributed Services*, Christopher Lesniewski-Laas, Bryan Ford, Jacob Strauss, M. Frans Kaashoek, and Robert Morris. 14th ACM Symposium on Computer and Communications Security (CCS), October 2007.
31. *Structured Streams: a New Transport Abstraction*, Bryan Ford. ACM SIGCOMM, August 2007.
32. *Persistent Personal Names for Globally Connected Mobile Devices*, Bryan Ford, Jacob Strauss, Chris Lesniewski-Laas, Sean Rhea, Frans Kaashoek, and Robert Morris. 7th USENIX Symposium on Operating Systems Design and Implementation (OSDI), November 2006.
33. *VXA: A Virtual Architecture for Durable Compressed Archives*, Bryan Ford. 4th USENIX Conference on File and Storage Technologies (FAST), December 2005.
34. *Peer-to-Peer Communication Across Network Address Translators*, Bryan Ford, Pyda Srisuresh, and Dan Kegel. USENIX Annual Technical Conference (USENIX), April 2005.
35. *Parsing Expression Grammars: A Recognition-Based Syntactic Foundation*, Bryan Ford. 31st ACM Symposium on Principles of Programming Languages (POPL), January 2004.
36. *Packrat Parsing: Simple, Powerful, Lazy, Linear Time*, Bryan Ford. International Conference on Functional Programming (ICFP), October 2002.
37. *Interface and Execution Models in the Fluke Kernel*, Bryan Ford, Mike Hibler, Jay Lepreau, Roland McGrath, and Patrick Tullmann. USENIX Symposium on Operating Systems Design and Implementation (OSDI), February 1999.
38. *The Flux OSKit: A Substrate for Kernel and Language Research*, Bryan Ford, Godmar Back, Greg Benson, Jay Lepreau, Albert Lin, and Olin Shivers. 16th ACM Symposium on Operating System Principles (SOSP), October 1997.
39. *Flick: A Flexible, Optimizing IDL Compiler*, Eric Eide, Kevin Frei, Bryan Ford, Jay Lepreau, Gary Lindstrom. ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), June 1997.
40. *Microkernels Meet Recursive Virtual Machines*, Bryan Ford, Mike Hibler, Jay Lepreau, Patrick Tullmann, Godmar Back, and Stephen Clawson. USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 1996.
41. *CPU Inheritance Scheduling*, Bryan Ford and Sai R. Susarla. USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 1996.
42. *Evolving Mach 3.0 to a Migrating Thread Model*, Bryan Ford and Jay Lepreau. USENIX Winter Technical Conference (USENIX), January 1994.
43. *In-Kernel Servers on Mach 3.0: Implementation and Performance*, Jay Lepreau, Mike Hibler, Bryan Ford, and Jeffrey Law. 3rd USENIX Mach Symposium, April 1993.

Refereed Workshop Publications

44. *Flash Freezing Flash Boys: Countering Blockchain Front-Running*, Haoqian Zhang, Louis-Henri Merino, Vero Estrada-Galiñanes, and Bryan Ford. Decentralized Internet, Networks, Protocols, and Systems (DINPS), July 2022.
45. *Immunizing Systems from Distant Failures by Limiting Lamport Exposure*, Cristina Băsescu and Bryan Ford. 20th ACM Workshop on Hot Topics in Networks (HotNets 2021), November 2021.
46. *Rethinking General-Purpose Decentralized Computing*, Enis Ceyhun Alp, Eleftherios Kokoris-Kogias, Georgia Fragkouli, and Bryan Ford. 17th Workshop on Hot Topics in Operating Systems (HotOS XVII), May 2019.

47. *MedChain: Accountable and Auditable Data Sharing in Distributed Clinical Research Networks*, Juan Ramón Troncoso-Pastoriza, Jean Louis Raisaro, Linus Gasser, Bryan Ford, and Jean-Pierre Hubaux. AMIA 2019 Informatics Summit, March 2019.

48. *MedCo: Enabling Privacy-Conscious Exploration of Distributed Clinical and Genomic Data*, Jean Louis Raisaro, Juan Ramón Troncoso-Pastoriza, Mickaël Misbach, João Sá Sousa, Sylvain Pradervand, Edoardo Missiaglia, Olivier Michielin, Bryan Ford, and Jean-Pierre Hubaux. *4th Workshop on Genome Privacy and Security (GenoPri'17)*, October 2017.

49. *Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies*, Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. IEEE Security & Privacy on the Blockchain (IEEE S&B), April 2017.

50. *Multiple Objectives of Lawful-Surveillance Protocols*, Joan Feigenbaum and Bryan Ford. 25th International Workshop on Security Protocols (SPW), March 2017.

51. *Privacy-Preserving Lawful Contact Chaining*, Aaron Segal, Joan Feigenbaum, and Bryan Ford. Workshop on Privacy in the Electronic Society (WPES), October 2016.

52. *PriFi: A Low-Latency and Tracking-Resistant Protocol for Local-Area Anonymous Communication*, Ludovic Barman, Mahdi Zamani, Italo Dacosta, Joan Feigenbaum, Bryan Ford, Jean-Pierre Hubaux, David Wolinsky. Workshop on Privacy in the Electronic Society (WPES), October 2016.

53. *Managing Identities Using Blockchains and CoSi*, Eleftherios Kokoris-Kogias, Linus Gasser, Ismail Khoffi, Philipp Jovanovic, Nicolas Gailly, Bryan Ford. 9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), July 2016.

54. *Certificate Cothority: Towards Trustworthy Collective CAs*, Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, and Bryan Ford. 8th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), July 2015.

55. *Catching Bandits and* Only *Bandits: Privacy-Preserving Intersection Warrants for Lawful Surveillance*, Aaron Segal, Bryan Ford, and Joan Feigenbaum. 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI), August 2014.

56. *From Onions to Shallots: Rewarding Tor Relays with TEARS*, Rob Jansen, Andrew Miller, Paul Syverson, and Bryan Ford. 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), July 2014.

57. *A TorPath to TorCoin: Proof-of-Bandwidth Altcoins for Compensating Relays*, Mainak Ghosh, Miles Richardson, and Bryan Ford. 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), July 2014.

58. *Crypto-Book: An Architecture for Privacy Preserving Online Identities*, John Maheswaran, David Isaac Wolinsky, and Bryan Ford. Twelfth ACM Workshop on Hot Topics in Networks (HotNets), November 2013.

59. *Conscript Your Friends into Larger Anonymity Sets with JavaScript*, Henry Corrigan-Gibbs and Bryan Ford. Workshop on Privacy in the Electronic Society (WPES), November 2013.

60. *Structural Cloud Audits that Protect Private Information*, Hongda Xiao, Bryan Ford, and Joan Feigenbaum. ACM Cloud Computing Security Workshop (CCSW), November 2013.

61. *An Untold Story of Redundant Clouds: Making Your Service Deployment Truly Reliable*, Ennan Zhai, Ruichuan Chen, David Isaac Wolinsky, and Bryan Ford. 9th Workshop on Hot Topics in Dependable Systems (HotDep), November 2013.

62. *Reducing Latency in Tor Circuits with Unordered Delivery*, Michael F. Nowlan, David Isaac Wolinsky, and Bryan Ford. 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI), August 2013.

63. *Lazy Tree Mapping: Generalizing and Scaling Deterministic Parallelism*, Yu Zhang and Bryan Ford. 4th Asia-Pacific Workshop on Systems (APSYS), July 2013.

64. *Welcome to the World of Human Rights: Please Make Yourself Uncomfortable*, Henry Corrigan-Gibbs and Bryan Ford. Cyber-security Research Ethics Dialog & Strategy Workshop (CREDS), May 2013.

65. *Scavenging for Anonymity with BlogDrop*, Henry Corrigan-Gibbs and Bryan Ford. Provable Privacy Workshop (ProvPriv), July 2012.

66. *Icebergs in the Clouds: the Other Risks of Cloud Computing*, Bryan Ford. 4th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud), June 2012.
67. *Plugging Side-Channel Leaks with Timing Information Flow Control*, Bryan Ford. 4th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud), June 2012.
68. *Non-Linear Compression: Gzip Me Not!*, Michael F. Nowlan and Bryan Ford. 4th USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage), June 2012.
69. *Scalable Anonymous Group Communication in the Anytrust Model*, David Isaac Wolinsky, Henry Corrigan-Gibbs, Bryan Ford, and Aaron Johnson. 5th European Workshop on Systems Security (EuroSec), April 2012.
70. *Faceless: decentralized anonymous group messaging for online social networks*, Xiaoxiao Song, David Isaac Wolinsky, and Bryan Ford. 5th Workshop on Social Network Systems (SNS), April 2012.
71. *A Virtual Memory Foundation for Scalable Deterministic Parallelism*, Yu Zhang and Bryan Ford. 2nd ACM SIGOPS Asia-Pacific Workshop on Systems (APSys), July 2011.
72. *CertiKOS: A Certified Kernel for Secure Cloud Computing*, Liang Gu, Alexander Vaynberg, Bryan Ford, Zhong Shao, and David Costanzo. 2nd ACM SIGOPS Asia-Pacific Workshop on Systems (APSys), July 2011.
73. *Deterministic OpenMP for Race-Free Parallelism*, Amittai Aviram and Bryan Ford. 3rd USENIX Workshop on Hot Topics in Parallelism (HotPar), May 2011.
74. *Workspace Consistency: A Programming Model for Shared Memory Parallelism*, Amittai Aviram, Bryan Ford, and Yu Zhang. 2nd Workshop on Determinism and Correctness in Parallel Programming (WoDet), March 2011.
75. *Minion—an All-Terrain Packet Packhorse to Jump-Start Stalled Internet Transports*, Janardhan Iyengar, Bryan Ford, Dishant Ailawadi, Syed Obaid Amin, Michael Nowlan, Nabin Tiwari, and Jeff Wise. 8th International Workshop on Protocols for Future, Large-Scale & Diverse Network Transports (PFLDNeT), November 2010.
76. *Determinating Timing Channels in Compute Clouds*, Amittai Aviram, Sen Hu, Bryan Ford, and Ramakrishna Gummadi. ACM Cloud Computing Security Workshop (CCSW), October 2010.
77. *An Efficient Cross-Layer Negotiation Protocol*, Bryan Ford and Janardhan Iyengar. 8th Workshop on Hot Topics in Networks (HotNets), October 2009.
78. *Device Transparency: a New Model for Mobile Storage*, Jacob Strauss, Chris Lesniewski-Laas, Justin Mazzola Paluska, Bryan Ford, Robert Morris, and Frans Kaashoek. SOSP Workshop on Hot Topics in Storage and File Systems (HotStorage), October 2009.
79. *Breaking Up the Transport Logjam*, Bryan Ford and Janardhan Iyengar. 7th Workshop on Hot Topics in Networks (HotNets), October 2008.
80. *An Offline Foundation for Online Accountable Pseudonyms*, Bryan Ford and Jacob Strauss. First International Workshop on Social Network Systems, April 2008.
81. *User-Relative Names for Globally Connected Personal Devices*, Bryan Ford, Jacob Strauss, Chris Lesniewski-Laas, Sean Rhea, Frans Kaashoek, and Robert Morris. 5th International Workshop on Peer-to-Peer Systems (IPTPS), February 2006.
82. *Unmanaged Internet Protocol: Taming the Edge Network Management Crisis*, Bryan Ford. 2nd Workshop on Hot Topics in Networks (HotNets), November 2003.
83. *The Flux OS Toolkit: Reusable Components for OS Implementation*, Bryan Ford, Jay Lepreau, Steve Clawson, Kevin Van Maren, Bart Robinson, and Jeff Turner. 6th IEEE Workshop on Hot Topics in Operating Systems (HotOS), May 1997.
84. *User-level Checkpointing through Exportable Kernel State*, Patrick Tullmann, Jay Lepreau, Bryan Ford, and Mike Hibler. 5th IEEE International Workshop on Object-Orientation in Operating Systems (IWOOOS), October 1996.
85. *The Persistent Relevance of the Local Operating System to Global Applications*, Jay Lepreau, Bryan Ford, and Mike Hibler. 7th ACM SIGOPS European Workshop, September 1996.

86. *Microkernels Should Support Passive Objects*, Bryan Ford and Jay Lepreau. 3rd IEEE International Workshop on Object-Orientation in Operating Systems (IWOOOS), December 1993.

87. *FLEX: A Tool for Building Efficient and Flexible Systems*, John B. Carter, Bryan Ford, Mike Hibler, Ravindra Kuramkote, Jeffrey Law, Jay Lepreau, Douglas B. Orr, Leigh Stoller, and Mark Swanson. 4th Workshop on Workstation Operating Systems (WWOS), October 1993.

Patents

88. *US20210018953A1: Asynchronous distributed coordination and consensus with threshold logical clocks*, Bryan Ford. July 14, 2020.

89. *WO2019158209A1: Methods and systems for secure data exchange*, Bryan Ford, Linus Gasser, Eleftherios Kokoris Kogias, and Philipp Jovanovic. February 16, 2018.

90. *US10581613B2: Cryptographically verifiable data structure having multi-hop forward and backwards links and associated systems and methods*, Bryan Ford, Linus Gasser, Eleftherios Kokoris Kogias, and Philipp Jovanovic. June 9, 2017.

91. *WO2018099577A1: System and method for providing a collective decentralized authority for sharing sensitive data*, Bryan Ford, Jean-Pierre Hubaux, Patricia Egger, Jean-Louis Raisaro, and Zhicong Huang. December 2, 2016.

92. *WO2018076013A1: Systems and method for anonymous, low-latencey, tracking-resistant communications in a networked environment*, Bryan Alexander Ford, Ludovic Barman, Jean-Pierre Hubaux, Italo Dacosta, and Joan Feigenbaum. October 21, 2016.

93. *US7706373B2: Session initiation and maintenance while roaming*, Richard H. Xu, Chong-Jin Koh, Bryan Ford, Markus Hahn, Gabriel Berryn Levy, Ching-Hai Tsai, Yusuf Saib, and Srinivasa Yarrakonda. November 1, 2006.

94. *US6938097B1: System for early packet steering and FIFO-based management with priority buffer support*, Paul B. Vincent and Bryan A. Ford. July 2, 1999.

Internet RFCs

95. *Unintended Consequences of NAT Deployments with Overlapping Address Space*, P. Srisuresh and B. Ford. RFC 5684, February 2010.

96. *NAT Behavioral Requirements for ICMP*, P. Srisuresh, B. Ford, S. Sivakumar, S. Guha. RFC 5508, April 2009.

97. *NAT Behavioral Requirements for TCP*, S. Guha, K. Biswas, B. Ford, S. Sivakumar, and P. Srisuresh. RFC 5382, October 2008.

98. *State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)*, Pyda Srisuresh, Bryan Ford, and Dan Kegel. RFC 5128, March 2008.

Technical Reports and Other Publications

99. *Auditing the Swiss Post E-voting System: An Architectural Perspective*, Bryan Ford. Swiss Federal Chancellery, E-voting: Results of the first independent examination available, April 2022.

100. *TRIP: Trustless Coercion-Resistant In-Person Voter Registration*, Louis-Henri Merino, Simone Colombo, Jeff Allen, Vero Estrada-Galiñanes, and Bryan Ford. arXiv preprint, February 2022.

101. *Design choices for Central Bank Digital Currency*, Sarah Allen, Srdjan Capkun, Ittay Eyal, Giulia Fanti, Bryan Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst, and Fan Zhang. Global Economy & Development Working Paper 140, Brookings Institution, July 2020.

102. *Scaling Software-Defined Network Controllers on Multicore Servers*, Andreas Voellmy, Bryan Ford, Paul Hudak, and Y. Richard Yang. Yale University Technical Report TR1468, July 2012.

103. *Strong Theft-Proof Privacy-Preserving Biometric Authentication*, Ewa Syta, Michael J. Fischer, Abraham Silberschatz, Gina Gallegos García, and Bryan Ford. Yale University Technical Report TR1455, May 25, 2012.
104. *Advanced Development of Certified OS Kernels*, Zhong Shao and Bryan Ford. Yale University Technical Report TR1436, July 15, 2010.
105. *UIA: A Global Connectivity Architecture for Mobile Personal Devices*, Bryan Ford. Ph.D. thesis, Massachusetts Institute of Technology, September 2008. Supervisor: Professor Frans Kaashoek
106. *Directions in Internet Transport Evolution*, Bryan Ford. IETF Journal, Volume 3 Issue 3, December 2007.
107. *Scalable Internet Routing on Topology-Independent Node Identities*, Bryan Ford. Technical Report MIT-LCS-TR-926, October 31, 2003.
108. *Packrat Parsing: a Practical Linear-Time Algorithm with Backtracking*, Bryan Ford. Master's thesis, Massachusetts Institute of Technology, September 2002. Supervisor: Professor Frans Kaashoek
109. *Using Annotated Interface Definitions to Optimize RPC*, Bryan Ford, Mike Hibler, and Jay Lepreau. Technical Report UUCS-95-014, March 1995.
110. *Separating Presentation from Interface in RPC and IDLs*, Bryan Ford, Mike Hibler, and Jay Lepreau. Technical Report UUCS-95-018, December 1994.
111. *Notes on Thread Models in Mach 3.0*, Bryan Ford, Mike Hibler, and Jay Lepreau. Technical Report UUCS-93-012, April 1993.

Broader Audience Publications

112. *Seeking Anonymity in an Internet Panopticon*, Joan Feigenbaum and Bryan Ford. *Communications of the ACM*, 58(10), October 2015.
113. *GPUfs: the case for operating system services on GPUs*, Mark Silberstein, Bryan Ford, and Emmett Witchel. *Communications of the ACM*, 57(12), December 2014.
114. *Technology Can Make Lawful Surveillance Both Open and Effective*, Bryan Ford and Joan Feigenbaum. MIT Technology Review, August 18, 2014.
115. *Is Data Hoarding Necessary for Lawful Surveillance?* Bryan Ford and Joan Feigenbaum. Huffington Post, April 19, 2014.
116. *An Open Letter from US Researchers in Cryptography and Information Security*. January 24, 2014.
117. *Efficient System-Enforced Deterministic Parallelism (Research Highlights)*, Amittai Aviram, Shu-Chun Weng, Sen Hu, and Bryan Ford. *Communications of the ACM* 55(5), May 2012.

Coverage in Popular Media

Building a new Tor that can resist next-generation state surveillance, J.M. Porup, arstechnica, August 31, 2016.

On Riffle: An Efficient Communication System With Strong Anonymity:

- Riffle is Tor's spiritual successor for next-gen anonymous networks, TelecomsTech, Ryan Daws, July 13, 2016.
- Meet Riffle, the next-gen anonymity network that hopes to trounce Tor, The Register, Iain Thomson, July 13, 2016.
- MIT Anonymity Network Riffle Promises Efficiency, Security, ThreatPost, Chris Brook, July 13, 2016.
- Riffle, le réseau anonyme qui veut supplanter Tor, 20 minutes, July 12, 2016.
- Riffle Is More Secure, and Less Useful, Than Tor, Inverse, Nathaniel Mott, July 12, 2016.
- Riffle is a new anonymous sharing technique 10 times faster than predecessors, the Inquirer, Chris Merriman, July 12, 2016.
- MIT Thinks It Can One-Up TOR With New Anonymity Network: Riffle, Hackaday, Mike Szczys, July 12, 2016.

– Riffle a new anonymity network by MIT is more secure than Tor, TechWorm, Kavita Iyer, July 12, 2016.
– MIT communication platform Riffle could surpass Tor in anonymity, International Business Times, India Ashok, July 12, 2016.
– MIT's Riffle is an anonymous network more secure than Tor, Firstpost, Aditya Madanapalle, July 12, 2016.
– MIT: Our Anonymity Network Riffle Is Better than Tor, Softpedia, Catalin Cimpanu, July 12, 2016.
– Researchers are developing an anonymity network more secure than Tor, dna India, July 12, 2016.
– New secure communication system plugs Tor's vulnerabilities, Engineering and Technology Magazine, Tereza Pultarova, July 12, 2016.
– MIT's New Anonymity Network Is Claimed to Be More Secure Than Tor, Gadgets360, Shekhar Thakran, July 12, 2016.
– After Tor exploit, researchers develop new anonymity network, SC Magazine, Jeremy Seth Davis, July 12, 2016.
– How To Stay Anonymous Online? Researchers At MIT's Computer Science And Artificial Intelligence Laboratory Are Working On A New Anonymity Scheme!, University Herald, Vinay Patel, July 12, 2016.
– MIT's anonymous online communications protocol Riffle could beat Tor at its own game, TechCrunch, Devin Coldewey, July 11, 2016.
– MIT anonymity network promises to be more secure than Tor, engadget, Jon Fingas, July 11, 2016.
– MIT Researchers Devise New Anonymity Network Following Tor Bug, PC Magazine, Angela Moscaritolo, July 11, 2016.
– Researchers tout new anonymity network, The Hill, Joe Uchill, July 11, 2016.
– MIT Researchers Create Secure, Fast Anonymity System, Campus Technology, Sri Ravipati, July 11, 2016.
– How to stay anonymous online, MIT News, July 11, 2016.

On Apple, FBI, and Software Transparency:

– Guest on *Justice Radio with Steven Rambam*, March 23, 2016.
– Guest on *Loud & Clear with Brian Becker*, March 22, 2016.
– *How Apple Could Fed-Proof Its Software Update System*, MIT Technology Review, Tom Simonite, March 11, 2016.
– *Apple fears gov't overreach, Cothority offers co. help*, SC Magazine, Teri Robinson, March 10, 2016.
– *Cothority offers to help Apple security with distributed cosigning*, MacNN, March 10, 2016.
– *Using distributed code-signatures to make it much harder to order secret backdoors*, BoingBoing, Cory Doctorow, March 10, 2016.
– *Cothority to Apple: Let's make secret backdoors impossible*, arstechnica UK, J.M. Porup, March 10, 2016.

Dragons and butterflies: The chaos of other people's clouds, The Register, Danny Bradbury, February 5, 2016.

Co-thority statt Authority: Viele-Augen-Prinzip für Zertifikate, Heise (Germany), Monika Ermert, November 5, 2015.

'Dissent,' a New Type of Security Tool, Could Markedly Improve Online Anonymity, Motherboard, J.M. Porup, September 16, 2015.

Inside Cyber Security: Experts Talk Tech, WPNR News program "Where We Live" with John Dankosky, January 13, 2015.

On ***mass surveillance***:

– *Yale profs propose openness, crypto for disciplined surveillance*, John Fontana. ZDNet, August 20, 2014.

- *Researchers say you can surveil everyone and see only the criminals*, Zach Wener-Fligner. Quartz, August 20, 2014.
- *Some of the biggest names in cryptography condemn NSA spying in open letter*, Andrea Peterson, January 24, 2014.
- *US crypto researchers to NSA: If you must track, track responsibly*, Nidhi Subbaraman, NBC News, January 27, 2014.

On ***The Dissent Project***:

- *Privacy, please: New technologies could hide your identity online*, Nidhi Subbaraman, NBC News, June 14, 2013.

Icebergs in the Clouds [HotCloud '12] covered by many journalists and tech bloggers including:

- *Detailed Questions Hit the Cloud*, Greg Goth, IEEE Internet Computing, Sep-Oct, 2012.
- *That Glorious Fireworks Fail Last Week? Imagine That's Your Data*, Edward Tenner, The Atlantic, July 13, 2012.
- *Amazon Web Services: The hidden bugs that made AWS' outage worse*, Jack Clark, Cloud Watch, July 3, 2012.
- *The Cloud, or a Monster on the Loose?*, Arthur Cole, ITBusinessEdge, June 11, 2012.
- *Cloudburst: Unexplored Risks of the Cloud*, Keith Dawson, Business Agility, April 4, 2012.
- *The Risk of a Meltdown In the Cloud*, Slashdot, March 20, 2012.

On ***Determinating Timing Channels in Compute Clouds*** paper [CCSW '10]:

- *Spotting Virtual Intruders*, Erica Naone, MIT Technology Review, March 9, 2011.

Industry Experience

Nuvoiz Inc. — Mountain View, CA
Consultant — 2006
Provided design assistance on NAT traversal technology for voice-over-IP communication.

Phobos Inc. (acquired by SonicWALL in 2000) — Salt Lake City, UT
Systems architect — 1998–2000
Designed high-speed traffic management hardware/software systems in a networking startup.

Sleepless Software — Salt Lake City, UT
Founder — 1993–1998
Developed and marketed entertainment products for MS-DOS, Windows, and Java platforms.

Open Software Foundation — Cambridge, MA
Consultant — 1993
Advised on integration of fast RPC and migrating threads into the OSF Mach kernel.

Hewlett-Packard — McMinnville, OR
Software engineer — summer 1992
Cardiology Business Unit: wrote database tools for an ECG management system.

Designing Minds — Logan, UT
Consultant — 1991–1992
Designed and wrote drivers for high-speed data compression hardware.

Waterford Institute — Provo, UT
Software engineer — summers 1989–1991
Created educational curricula and software with a team of teachers and programmers,

Designing Minds — Logan, UT
Consultant — 1987–1988
Developed a painting program for bitmapped graphics and animation on the Amiga, titled *Chroma Paint*, published 1988.

Software Artifacts Publicly Released

2015 Cothority: scalable collective authority prototype.

2012 Dissent: an accountable anonymous group communication system. Open source release.

2010 Determinator/PIOS: an experimental research/instructional operating system. Open source release.

2007 SST: an experimental transport protocol implemented as a C++ library. Open source release.

2005 UIA: a naming and routing protocol suite for personal mobile devices. Open source release.

2005 vx32: an application-level virtual machine/sandbox for x86. Open source release.

2002 Pappy: a packrat parser generator for Haskell. Open source release.

1999 Fluke: an experimental microkernel operating system. Open source release.

1998 Flux OSKit: a component library for operating system construction. Open source release.

1997 Flick: an optimizing Interface Definition Language (IDL) compiler. Open source release.

1995 Inner Worlds: a side-scrolling action/adventure game. Released as Shareware by Sleepless Software.

1993 Migrating Threads: an enhancement to Mach 3.0, later incorporated in OSF Mach and Mac OS X.

1989 MultiPlayer: a multi-format music player for Amiga computers. Released as Shareware by author.

1988 Chroma Paint: a bitmapped graphics tool for Amiga. Commercially published by Designing Minds.