

ANDREW MILLER

1308 W Main St. / Urbana, IL 61820 / soc1024@illinois.edu / (234) 421-1024 / <http://soc1024.ece.illinois.edu/>

I am an Assistant Professor in the Electrical and Computer Engineering department at the University of Illinois, Urbana-Champaign. My research interests lie at the intersection of computer security, programming languages, and distributed systems. My current focus is in building secure decentralized systems, such as cryptocurrencies.

APPOINTMENTS

2016 - Present: Assistant Professor, Electrical and Computer Engineering department, University of Illinois at Urbana-Champaign

EDUCATION

2013-2016: Ph.D. in Computer Science, University of Maryland

2009-2012: M.S. in Computer Science, University of Central Florida

2005-2009: B.S. in Computer Science, University of Central Florida

SELECTED PUBLICATIONS

hbACSS: How to Robustly Share Many Secrets Thomas Yurek, Licheng Luo, Jaiden Fairoze, Aniket Kate, and Andrew Miller. **NDSS 2022** (to appear).

Practical Asynchronous Distributed Key Generation. Sourav Das, Tom Yurek, Zhuolun Xiang, Andrew Miller, Lefteris Kokoris-Kogias, Ling Ren. IEEE Symposium on Security and Privacy 2022 (to appear).

Publicly Auditable MPC-as-a-Service with succinct verification and universal setup Sanket Kanjalkar, Ye Zhang, Shreyas Gandlur, Andrew Miller. IEEE Workshop on Security and Privacy on the Blockchain, 2021.

An Empirical Analysis of Privacy in the Lightning Network George Kappos, Haaron Yousaf, Ania Piotrowska, Sanket Kanjalkar, Sergi Delgado-Segura, Andrew Miller, Sarah Meiklejohn. Financial Crypto 2021.

Safer Illinois and RokWall: Privacy Preserving University Health Apps for COVID-19. Vikram Sharma Mailthody, James Wei, Nicholas Chen, Mohammad Behnia, Ruihao Yao, Qihao Wang, Vedant Agrawal, Churan He, Lijian Wang, Leihao Chen, Amit Agarwal, Edward Richter, Wen-Mei Hwu, Christopher W. Fletcher, Jinjun Xiong, Andrew Miller, Sanjay Patel. Workshop on Secure IT Technologies against COVID-19 (CoronaDef) 2021.

CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability Deepak Maram and Harjasleen Malvai and Fan Zhang and Nerla Jean-Louis and Alexander Frolov and Tyler Kell and Tyrone Lobban and Christine Moy and Ari Juels and Andrew Miller. **(IEEE S&P 2021)**

Non-interactive Proofs of Proof-of-Work. Aggelos Kiayias, Andrew Miller, Dionysis Zindros. Financial Cryptography 2020

Custos: Practical Tamper-Evident Auditing of Operating Systems Using Trusted Execution. Riccardo Paccagnella, Pubali Datta, Wajih Ul Hassan, Adam Bates, Christopher W. Fletcher, Andrew Miller, Dave Tian. NDSS 2020

Pisa: Arbitration Outsourcing for State Channels. Patrick McCorry, Surya Bakshi, Iddo Bentov, Sarah Meiklejohn, Andrew Miller. ACM Advances in Financial Technology, 2019.

HoneyBadgerMPC and AsynchroMix: Practical AsynchronousMPC and its Application to Anonymous Communication. Donghang Lu, Thomas Yurek, Samarth Kulshreshtha, Rahul Govind, Rahul Mahadev, Aniket Kate, Andrew Miller. CCS 2019.

ILC: a calculus for composable, computational cryptography. Kevin Liao, Matthew Hammer, and Andrew Miller. **PLDI 2019**

Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution. Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah Johnson, Ari Juels, Andrew

Miller, Dawn Song. EuroS&P 2019

TxProbe: Discovering Bitcoin's Network Topology Using Orphan Transactions. Sergi Delgado-Segura, Surya Bakshi, Cristina Pérez-Solà, James Litton, Andrew Pachulski, Andrew Miller, and Bobby Bhattacharjee. FC 2019

Sprites and State Channels: Payment Networks that Go Faster than Lightning. Andrew Miller, Iddo Bentov, Surya Bakshi, Ranjit Kumaresan, and Patrick McCorry. FC 2019

Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees. Giulia Fanti, Surya Bakshi, Shaileshh Bojja Venkatakishnan, Andrew Miller, Bradley Denby, Shruti Bhargava, Pramod Viswanath. ACM SIGMETRICS 2018.

DelegaTEE: Brokered Delegation Using Trusted Execution Environments Sinisa Matetic and Moritz Schneider and Andrew Miller and Ari Juels and Srdjan Capkun. **USENIX Security 2018**.

Erays: Reverse Engineering Ethereum's Opaque Smart Contracts. Yi Zhou, Deepak Kumar, Surya Bakshi, Joshua Mason, Andrew Miller, and Michael Bailey, University of Illinois, Urbana-Champaign. USENIX Security 2018.

An Empirical Analysis of Traceability in the Monero Blockchain. Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin. **PETS 2018**

Instantaneous Decentralized Poker. Iddo Bentov, Ranjit Kumaresan, and Andrew Miller. **AsiaCrypt 2017**.

The Honey Badger of BFT Protocols. Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. **CCS 2016**

Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, Charalampos Papamanthou. IEEE Security & Privacy (Oakland), May 2016.

SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten. IEEE Security & Privacy (Oakland), May 2015.

Permacoin: Repurposing Bitcoin Work for Long-Term Data Preservation. Andrew Miller, Ari Juels, Elaine Shi, Bryan Parno, Jonathan Katz. IEEE Security & Privacy (Oakland), May 2014.

Non-outsourcable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions. Andrew Miller, Elaine Shi, Ahmed Kosba, and Jonathan Katz. ACM Computer and Communications Security (CCS), October 2015.

AWARDS

- 2021: NSF CAREER Award 1943499

- 2018: IEEE S&P Distinguished Reviewer

- 2017: University of Maryland, Larry S. Davis Doctoral Dissertation Award

GRADUATE STUDENT ADVISEES

Surya Bakshi - 5th year PhD, prelim scheduled for May

Tom Yurek - 5th year PhD, prelim scheduled for May

Yunqi Li - 3rd year PhD

Nerla Jean-Louis - 2nd year PhD

Bolton Bailey - 2nd year PhD

Amit Agarwal (coadvised with Dakshita Khurana) - 3rd year PhD

INVITED LECTURES

2020 April - Invited Lecture at Purdue University
2022 May - Invited talk at PLCrypto Workshop
2022 June - Keynote at 4th Blockchain Technology Symposium

SERVICE

Program Committees:

IEEE Security and Privacy:	2017, 2018, 2019
ACM CCS	2017, 2019, 2022
Financial Cryptography	2017,2018,2019,2020,2021,2022
NDSS	2017
Usenix Security	2017, 2021
Advances in Financial Technology	2020

Steering Committee:

Financial Cryptography	2018-2022
------------------------	-----------

Program committee chair:

4th Bitcoin Research Workshop	2017
-------------------------------	------