

Aniket Kate

Department of Computer Science
Purdue University
<https://www.cs.purdue.edu/homes/akate/>
aniket@purdue.edu

305 N. University Street
West Lafayette, IN 47907
USA 47907
Office: +1-765-496-2763

EDUCATION

Date: *August 22, 2024*

- Ph.D., Computer Science, University of Waterloo, Canada, 2010
Advisor: Ian Goldberg
- M.Tech., Computer Science and Engineering, Indian Institute of Technology–Bombay, India, 2006
- B.E., Information Technology, Mumbai University, India, 2003

RESEARCH INTEREST

I am an applied cryptographer and a privacy researcher. My research builds on and expands applied cryptography, distributed computing, and game theory toward developing and analyzing robust solutions for privacy and (distributed) trust. My current research projects focus on distributed ledgers (or blockchains), distributed cyber-physical systems (CPS), and privacy-preserving computation and communication.

In my group, (i) We enhance the security, privacy, and scalability of distributed ledgers and communication across Web2 and Web3 systems, and devise their novel crypto-economic applications to the decentralized finance, distributed CPS, and beyond; (ii) We design and analyze efficient, provably secure cryptographic solutions for privacy-preserving computation and network anonymity, and formalize and realize privacy and censorship resistance for emerging communication modalities.

EXPERIENCE

- Computer Science, Purdue University
Associate Professor
West Lafayette, IN, USA
Aug 2020–*present*
- Supra Labs Inc.
Chief Research Officer
May 2022–*present*
- Computer Science, Purdue University
Assistant Professor
West Lafayette, IN, USA
Aug 2015–*Aug 2020*
- Cluster of Excellence, Saarland University
Junior Faculty Member, Independent Research Group Leader
Saarbruecken, Germany
Aug 2012–*Sep 2015*
- Max Planck Institute for Software Systems (MPI-SWS)
Postdoctoral Researcher with Michael Backes
Saarbruecken, Germany
Sep 2010–July 2012
- University of Waterloo
Research Assistant with Ian Goldberg
Waterloo, Canada
May 2007–Aug 2010
- Research Assistant with Urs Hengartner
Sep 2006–Apr 2007

AWARDS AND HONORS

INTERNAL TO PURDUE

- ◇ University Faculty Scholar 2024–2029.
- ◇ Purdue Seed for Success award, 2019.
- ◇ College of Science Faculty Team Award, February 2016.

EXTERNAL TO PURDUE

- ◇ Sui Academic Research Award, August 2024.
- ◇ National Science Foundation (NSF) CAREER Award, February 2019.
- ◇ Cyber Security Awareness Week (CSAW) Applied Research Award (Top-10) Finalist, November 2017.
- ◇ Best paper award at ACM Conference on Online Social Networks (COSN), November 2015.
- ◇ David R. Cheriton Graduate Scholarship, University of Waterloo, 2007–2010.

ENGAGEMENT AND SERVICE

DEPARTMENTAL ENGAGEMENT

- ◇ Started the Crypto Reading Group, (weekly meetings), Attendance: 20 graduate students and faculty members, Spring 2016–Spring 2020
- ◇ Committees
 - Member of the Graduate Admissions committee, 2015–2018, 2025
 - Member of the Security Faculty Search committee, 2018–2019
 - Member of the Graduate Student Board Advisor committee, 2018–2020
 - Member of the Graduate Study committee, 2019–2020
 - Member of the Colloquia committee, 2019–2020
 - Member of the Awards committee, 2020–2021
- ◇ Presentation for engagement seminars
 - CS 591: Research Seminar for Graduate Students, 2017, 2018, 2019.
 - Corporate Partner Meeting: Fall 2017.

COLLEGE-LEVEL ENGAGEMENT

- ◇ Offered a lecture as part of Global Science Leadership Seminar, College of Science, Fall 2018.

UNIVERSITY-LEVEL ENGAGEMENT

- ◇ Participating in the Future Mentors Program at John Martinson Honors College, Purdue University with graduate student Zhongtang Luo, 2024-25.
- ◇ A seminar on “Decentralized Web aka Web3” at Early Stage VC Symposium, Burton D. Morgan Center for Entrepreneurship, Apr 2022.
- ◇ A seminar on “Privacy and Accountability at International Sporting Events” at the (virtual) International Olympic Committee Cybersecurity Summit, Oct 2021.
- ◇ Organizing Committee Member for the “Big Data, Safe Food” Conference, 2020.
- ◇ Started the Blockchain Research meetings, (weekly meetings). Attendance: 15 graduate/undergraduate students across the campus, Fall 2016–Fall 2019
- ◇ Security Applications (IE 590): Purdue Online Learning (1 lecture on Blockchain Applications), Fall 2018
- ◇ the ONR STEM course (a lecture on Cyber Security every year), 2017-18. Also helped in preparing the online version of the course: CNIT 581
- ◇ Industry Engagement Talk for CERIAS and Purdue University’ Office of Corporate & Global Partnerships: Airbus (2024), German DFG Delegation (2023), Monsanto (2018), Master Card (2018), ARL (2018), Raytheon (2018), KAR (2018), SRC (2018), John Deere (2017), Intel (2017).
- ◇ Member, Interdisciplinary Graduate Program in Information Security (INSC) Admission Committee, CERIAS, Purdue University, 2016
- ◇ Introduction to blockchains, Research Seminar Series, School of Industrial Engineering, September 2017

PROFESSIONAL SERVICE

- ◇ Tenure Recommendation Letters: 2022 (1), 2023 (1)
- ◇ Editorial Board:
 - ACM Transactions on Privacy and Security (TOPS) 2024-*present*
 - Proceedings on Privacy Enhancing Technologies (PoPETS) 2018-2019
- ◇ Workshop Organizer:
 - Advances in Blockchains and Distributed Trust, IIT-Bombay, India, December 2024
 - Dagstuhl Seminar #24362: Next-Generation Secure Distributed Computing, Germany, June 2024
 - Workshop on Decentralized Credit Networks, Affiliated with Advances in Financial Technologies (AFT), Princeton, USA, Oct 2023

- (Virtual) Workshop on Blockchains + Economics (<https://blockchainsplusx.github.io/>), Aug 2023
- (Virtual) Workshop on Blockchains + TEEs (<https://blockchainsplusx.github.io/>), Mar 2023
- Workshop on Real-World Decentralized Cryptography, Affiliated with Real-World Crypto Symposium, Jan 2021
- ◇ Track Chair on Blockchain, IEEE Computer Security Foundations (CSF) 2019, 2022
- ◇ Technical Program Area Chair, IEEE Conference on Communications and Network Security (CNS) 2019
- ◇ Poster/Demo co-Chair, ACM Computer and Communication Security (CCS) 2016
- ◇ Proceedings co-Chair, ACM Computer and Communication Security (CCS) 2018
- ◇ Selected Program Committee Membership:
 - IEEE Symposium on Security and Privacy 2019-21, 2023-25.
 - Financial Cryptography and Data Security (FC) 2016, 2019-24.
 - ACM Computer and Communication Security (CCS) 2017-19, 2021-22, 2024.
 - Science of Blockchain Conference (SBC) 2024.
 - The Web Conference (WWW) 2013, 2019, 2021.
 - Usenix Security Symposium 2018, 2020-21.
 - ACM Advances in Financial Technologies (AFT) 2021-22.
 - ACM ASIA Conference on Computer and Communications Security (ASIACCS) 2021.
 - Crypto Valley Conference 2020-21.
 - Network and Distributed System Security Symposium (NDSS) 2018-19.
 - IEEE Computer Security Foundations (CSF) 2017, 2019, 2022.
 - ACM Workshop on Privacy in the Electronic Society (WPES) 2012, 2015, 2017, 2018, 2020.
 - International Conference on Privacy, Security, and Trust (PST) 2017.
 - Principles of Security and Trust (POST) 2017.
 - Advances in Cryptology—Eurocrypt 2016.
 - IEEE International Conference on Distributed Computing Systems (ICDCS) 2015-18, 2022.
 - The Bitcoin Workshop 2016-18.
 - International Conference on Applied Cryptography and Network Security (ACNS) 2016-18.
 - ACM Cloud Computing Security Workshop (CCSW) 2015.
 - ACM Cyber-Physical System Security Workshop (CPSS) 2015.
 - IEEE International Conference on Cloud Computing Technology and Science (CloudCom) 2015.
 - International Conference on Provable Security (ProvSec). 2014-15.
- ◇ NSF SaTC Panelist (In-person / Virtual, One panel/year), 2016-18
- ◇ NSF External Reviewer (multiple/year), 2018-20, 2022
- ◇ Mentor, NSF SaTC Aspiring PI workshop 2024, Chicago, USA, 2024
- ◇ Industrial Advisor: Deuro (2018-19), Keyless (2018), Torus (2019), Supra Labs (2021-22)

DIVERSITY ACTIVITIES

- ◇ Part of CERIAS center's Ukrainian Cyber-security Curriculum Development Project, May-Oct 2021
- ◇ Invited Talk, Black Graduate Student Association, Purdue University, February 2018 (Attended by more than 20 students from diverse international backgrounds)
- ◇ Hosted female students
 - Alejandra Ospina (Ecuador), as part of the Go-boiler program, August-February 2024-25
 - Karol Mejia (Colombia), as part of Colombia Purdue Partnership, August-December 2021
 - Lizzy Tengana Hurtado (Columbia) as part of Purdue's UREP-C program, June-December 2018
 - Durga Keerthi Mandarapu (India) as part of the GoBoiler internship program, Summer 2018 joined our Ph.D. program in Fall 2019
 - Christiane Kuhn (Germany), Fall 2019

- Jing Wen (China), Summer 2017

OTHER ACTIVITIES

- ◇ Invited to 2021 Japan-America Frontiers of Engineering (JAFOE) Symposium, National Academy of Engineering, USA, June 2021 (virtual)
- ◇ Research Group Leaders' Representative at Cluster of Excellence Board, Saarland University, 2013-15.
- ◇ Graduate Students' Representative at Director Search Committee, School of Computer Science, University of Waterloo, 2009-10.
- ◇ Cryptography Seminar Organizer for the Centre for Applied Cryptographic Research (CACR), University of Waterloo, Spring 2008.
- ◇ Overall Coordinator for Annual Network Security (SecNet 2006) Workshop, IIT-Bombay, Spring 2006

TEACHING EXPERIENCE

TEACHING ASSIGNMENTS

Purdue University

(CS 528) Network Security (3 credits, online+in-person)	Spring 2025
(CS 528) Network Security (3 credits, 27 students)	Spring 2022
(CS 59100 - RS1) Res Sem First Yr Gr Student (1 credit, 110 students)	Fall 2021
(CS 528) Network Security (3 credits, 14 students)	Spring 2021
(CS 426) Computer Security (3 credits, 58 students)	Fall 2020
(CS 59100 - RS1) Res Sem First Yr Gr Student (1 credit, 41 students)	Fall 2020
(CS 590-BTS) Blockchains & Cryptocurrencies (3 credits, 05 students)	Spring 2020
(CS 426) Computer Security (3 credits, 58 students)	Fall 2019
(CS 528) Network Security (3 credits, 21 students)	Spring 2019
(CS 590-BTS) Blockchains & Cryptocurrencies (New course , 3 credits, 14 students)	Spring 2019
(CS 528) Network Security (3 credits, 27 students)	Spring 2018
(CS 426) Computer Security (3 credits, 44 students)	Fall 2017
(CS 591) CERIAS Security Seminar (1 credit, 18 students)	Spring 2017
(CS 528) Network Security (Reworked, 3 credits, 06 students)	Spring 2017
(CS 426) Computer Security (Significantly redesigned, 3 credits, 41 students)	Fall 2016
(CS 528) Network Security (New course , 3 credits, 13 students)	Spring 2016
(CS 690-PET) Hot Topics in Privacy Enhancing Technologies (3 credits, 07 students+audits)	Fall 2015

Saarland University

Advanced Course: Applied Cryptography	Winter 2014/15
Seminar: Practical Cryptographic Systems	Winter 2012/13, Summer 2014
Advanced Course: Privacy Enhancing Technologies (co-taught)	Summer 2013, 2014, 2015

OTHER CONTRIBUTIONS TO UNDERGRADUATE EDUCATION

- Seminar Talk on Cryptography, CS 197 Freshman Honors Seminar. Spring 2017, 2018, 2023-24.
- Seminar Talk on Computer Security and Privacy Research, CS 397 Honors Seminar. Fall 2015-16, 2019, 2022-23.
- Invited Lecture on for Global Science Leadership Seminar (SCI 19500), Fall 2018.
- Invited Talk on Blockchains, BoilerMake Hackathon 2017. September 2017.
- Introducing Research to Undergraduate. Summer 2016–present
09 undergraduate students (06 from Purdue and 03 from outside)
- CS39000: Individual Study courses, undergraduate research assistants, and NSF REU

REFEREED PUBLICATIONS

Note: * indicates primary author, ^P denotes author who is postdoctoral researcher (or on other pre-faculty position) at the time of writing. ^U and ^G similarly indicate authors who were undergraduate and graduate students respectively at the time of writing. Publications with previous mentors are distinguished by the ^M tag.

JOURNAL ARTICLES

- 1 Nibesh Shrestha^{*}, Adithya Bhat^G, Aniket Kate, and Kartik Nayak. Synchronous distributed key generation without broadcasts *IACR Communications in Cryptology*, Vol. 01, no. 2, 2024.
- 2 Easwar V Mangipudi^{*G}, Krutarth R Rao^U, Jeremy Clark, and Aniket Kate. Pepal: Penalizing Multimedia Breaches and Partial Leakages *International Journal of Information Security*, Vol. 23, 447–465, 2024.
- 3 Donghang Lu^{*G} and Aniket Kate. RPM: Robust Anonymity at Scale. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2023(2), 2023.
- 4 Debajyoti Das^{*G}, Easwar Vivek Mangipudi^{*G}, and Aniket Kate. OrgAn: Organizational Anonymity with Low Latency. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2022(3), 2022.
- 5 Donghang Lu^{*G}, Albert Yu^G, Aniket Kate and Hemanta Maji. Polymath: Low-Latency MPC via Secure Polynomial Evaluations and its Applications. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2022(1), 2022.
- 6 Debajyoti Das^{*G}, Sebastian Meiser, Esfandiar Mohammadi, and Aniket Kate. Comprehensive Anonymity Trilemma: User Coordination is not enough. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2020(3), 356–383, 2020.
- 7 Mohsen Minaei^{*G}, Pedro Moreno-Sanchez^{*G}, and Aniket Kate. MoneyMorph: Censorship Resistant Rendezvous using Permissionless Cryptocurrencies. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2020(1), 404–424, 2020.
- 8 Duc Le^{*G}, Lizzy Tengana Hurtado^U, Adil Ahmad, Mohsen Minaei^G, Byoungyoung Lee, and Aniket Kate. A Tale of Two Trees: One Writes, and Other Reads. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2020(2), 519–536, 2020.
- 9 Mohsen Minaei^{*G}, Mainack Mondal^P, Patrick Loiseau, Krishna Gummadi, and Aniket Kate. Lethe: Conceal Content Deletion from Persistent Observers. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2019(1), 206–226, 2019.
- 10 Pedro Moreno-Sanchez^{*G}, Uzair Mahmood^G, and Aniket Kate. ClearChart: Ensuring Integrity of Consumer Ratings in Online Marketplaces. *Computers & Security Journal (CoSe)*, 78: 90–102, 2018.
- 11 Pedro Moreno-Sanchez^{*G}, Tim Ruffing^G, and Aniket Kate. PathShuffle: Credit Mixing and Anonymous Payments for Ripple. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2017 (3), 2017.
- 12 Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi. AnoA: A Framework for Analyzing Anonymous Communication Protocols. *Journal of Privacy and Confidentiality (JPC)*, 7(2): 79–125, 2016.
- 13 Pedro Moreno-Sanchez^{*}, Muhammad Bilal Zafar^G, and Aniket Kate. Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2016(4), 2016.
- 14 Michael Backes, Niklas Grimm^{*U}, and Aniket Kate. Data Lineage in Malicious Environments. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 13(2): 178–191, 2016. [Pre-Purdue Hire]
- 15 Maxwell Young^{*}, Aniket Kate, Ian Goldberg, and Martin Karsten. Towards Practical Communication in Byzantine-Resistant DHTs.^M *IEEE/ACM Transactions on Networking (ToN)*, 21(1), 2013.
- 16 Aniket Kate^{*} and Ian Goldberg. Generalizing Cryptosystems Based on the Subset Sum Problem.^M *Springer International Journal of Information Security (IJIS)*, 10 (3), 2011.
- 17 Aniket Kate^{*}, Gregory M. Zaverucha, and Ian Goldberg. Pairing-Based Onion Routing with Improved Forward Secrecy.^M *ACM Transactions on Information and System Security (TISSEC)*, 13(4), 2010.

CONFERENCE PUBLICATIONS

- 18 Yanxue Jia^{*P}, Varun Madathil, and Aniket Kate. HomeRun: High-efficiency Oblivious Message Retrieval, Unrestricted. *To appear at 29th ACM Conference on Computer and Communications Security (CCS)*, Oct 2024.
- 19 Akhil Bandarupalli^{*G}, Adithya Bhat, Saurabh Bagchi, Aniket Kate, and Michael Reiter. HashRand: Efficient Asynchronous Random Beacon without Threshold Cryptographic Setup. *To appear at 29th ACM Conference on Computer and Communications Security (CCS)*, Oct 2024.

- 20 Aniket Kate, Easwar Mangipudi, Pratyay Mukherjee, Hamza Saleem, and Sri Aravinda Krishnan Thyagarajan. Non-interactive VSS using Class Groups and Application to DKG. *To appear at 29th ACM Conference on Computer and Communications Security (CCS)*, Oct 2024.
- 21 Albert Yu^{*G}, Hai H. Nguyen^P, Aniket Kate, and Hemanta K. Maji. Unconditional Security using (Random) Anonymous Bulletin Board. *IEEE International Symposium on Information Theory (ISIT)*, Jul 2024.
- 22 Debajyoti Das^{*G}, Sebastian Meiser, Esfandiar Mohammadi, and Aniket Kate. Divide and funnel: a scaling technique for mix-networks. *IEEE Computer Security Foundations Symposium (CSF)*, Jul 2024.
- 23 Akhil Bandarupalli^{*G}, Adithya Bhat^G, Saurabh Bagchi, Aniket Kate, Chen-Da Liu-Zhang, and Michael K. Reiter. Delphi: Efficient Asynchronous Approximate Agreement for Distributed Oracles. *54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Jun 2024.
- 24 Akhil Bandarupalli^{*G}, Adithya Bhat, Somali Chaterji, Michael K. Reiter, Aniket Kate, and Saurabh Bagchi. SensorBFT: Fault-Tolerant Target Localization using Voronoi Diagrams and Approximate Agreement. *44th IEEE International Conference on Distributed Computing Systems (ICDCS)*, Jul 2024.
- 25 Tiantian Gong^{*G}, Ryan Henry, Alexandros Psomas, and Aniket Kate. More is Merrier: Relax the Non-Collusion Assumption in Multi-Server PIR. *44th IEEE Symposium on Security and Privacy (S&P (Oakland))*, May 2024.
- 26 Zhongtang Luo^{*G}, Adithya Bhat^G, Kartik Nayak, and Aniket Kate. Attacking and Improving the Tor Directory Protocol. *44th IEEE Symposium on Security and Privacy (S&P (Oakland))*, May 2024.
- 27 Jianting Zhang^{*G}, Wuhui Chen, Sifu Luo, Tiantian Gong^G, Zicong Hong, and Aniket Kate. Front-running Attack in Sharded Blockchains and Fair Cross-shard Consensus. *Network and Distributed System Security Symposium (NDSS)*, Feb 2024.
- 28 Adithya Bhat^{*G}, Akhil Bandarupalli^G, Manish Nagaraj, Saurabh Bagchi, Aniket Kate, and Michael K. Reiter. EESMR: Energy Efficient BFT-SMR for the masses. *ACM/IFIP International Middleware Conference (Middleware)*, Dec 2023.
- 29 Easwar Mangipudi^{*G}, Udit Desai, Mohsen Minaei, Mainack Mondal, and Aniket Kate. Uncovering Impact of Mental Models towards Adoption of Multi-device Crypto-Wallets. *28th ACM Conference on Computer and Communications Security (CCS)*, Nov 2023.
- 30 Aniket Kate, Easwar Mangipudi, Siva Maradana, and Pratyay Mukherjee. FlexiRand: Output Private (Distributed) VRFs and Application to Blockchains. *28th ACM Conference on Computer and Communications Security (CCS)*, Nov 2023.
- 31 Easwar Mangipudi^{*G}, Donghang Lu^G, Alexandros Psomas and Aniket Kate. Collusion-Deterrent Threshold Information Escrow. *IEEE Computer Security Foundations Symposium (CSF)*, Jul 2023.
- 32 Albert Yu^{*G}, Donghang Lu^G, Aniket Kate, and Hemanta K. Maji. SIM: Secure Interval Membership Testing and Applications to Secure Comparison. *IEEE European Symposium on Security and Privacy (Euro S&P)*, Jun 2023.
- 33 Prasanth Chakka, Saurabh Joshi, Aniket Kate, Joshua Tobkin and David Yang. DORA: Distributed Oracle Agreement with Simple Majority.^M *43rd International Conference on Distributed Computing Systems (ICDCS)*, Jun 2023
- 34 Adithya Bhat^{*G}, Akhil Bandarupalli^G, Saurabh Bagchi, Aniket Kate, and Michael K. Reiter. The Unique Chain Rule and its Applications. *Financial Cryptography and Data Security (FC)*, May 2023.
- 35 Adithya Bhat^{*G}, Nibesh Shrestha^{*}, Aniket Kate, and Kartik Nayak. OptRand: Optimistically Responsive Reconfigurable Distributed Randomness. *Network and Distributed System Security Symposium (NDSS)*, Mar 2023.
- 36 Lukas Aumayr, Pedro Moreno-Sanchez, Aniket Kate, and Matteo Maffei. Breaking and Fixing Virtual Channels: Domino Attack and Donner. *Network and Distributed System Security Symposium (NDSS)*, Mar 2023.
- 37 Easwar Mangipudi^{*G} and Aniket Kate. D-KODE: Distributed Mechanism to Manage a Billion Discrete-log Keys. *ACM Advances in Financial Technologies (AFT)*, Sep 2022.
- 38 Mohsen Minaei^{*G}, Mainack Mondal, and Aniket Kate. Empirical Understanding of Deletion Privacy: Experiences, Expectations, and Measures. *USENIX Security Symposium (Usenix SEC)*, Aug 2022.

- 39 Tiantian Gong^{*G}, Mohsen Minaei^G, Wenhai Sun, and Aniket Kate. Towards Overcoming the Undercutting Problem. 26th International Conference on Financial Cryptography and Data Security (FC), May 2022.
- 40 Thomas Yurek, Licheng Luo, Jaiden Fairoze, Aniket Kate, and Andrew Miller. hbACSS: How to Robustly Share Many Secrets . Network and Distributed System Security Symposium (NDSS), Feb 2022.
- 41 Sri Aravinda Krishnan Thyagarajan^{*}, Adithya Bhat^G, Tiantian Gong^G, Aniket Kate, and Dominique Schroeder. OpenSquare: Decentralized Repeated Modular Squaring Service. 28th ACM Conference on Computer and Communications Security (CCS), Nov 2021.
- 42 Adithya Bhat^{G*}, Nibesh Shrestha^{*}, Zhongtang Luo^U, Aniket Kate, and Kartik Nayak. RandPiper - Reconfiguration-Friendly Random Beacons with Quadratic Communication. 28th ACM Conference on Computer and Communications Security (CCS), Nov 2021.
- 43 Lukas Aumayr^{*}, Pedro Moreno-Sanchez, Aniket Kate, and Matteo Maffei. Blitz: Secure Multi-Hop Payments Without Two-Phase Commits. USENIX Security Symposium (Usenix SEC), Aug 2021.
- 44 Sri Aravinda Krishnan Thyagarajan^{*}, Adithya Bhat^{*G}, Bernardo Magri, Daniel Tschudi, and Aniket Kate. Reparó: Publicly Verifiable Layer to Repair Blockchains. 25th International Conference on Financial Cryptography and Data Security (FC), Feb 2021.
- 45 Mohsen Minaei^{*G}, S Chandra Mouli, Mainack Mondal, Bruno Ribeiro, and Aniket Kate. Cloaking Large-Scale Damaging Deletions on Social Platforms. Network and Distributed System Security Symposium (NDSS), Feb 2021.
- 46 Sri Aravinda Krishnan Thyagarajan^{*G}, Adithya Bhat^G, Giulio Malavolta, Nico Doettling, Aniket Kate, and Dominique Schroeder. Verifiable Timed Signatures Made Practical. 27th ACM Conference on Computer and Communications Security (CCS), Nov 2020.
- 47 Venkat Arun^{*U}, Aniket Kate, Deepak Garg, Peter Druschel, and Bobby Bhattacharjee. Finding Safety in Numbers with Secure Allegation Escrows. Network and Distributed System Security Symposium (NDSS), Feb 2020. (17% acceptance rate)
- 48 Pedro Moreno-Sanchez^{*}, Randomrun, Duc Le^G, Sarang Noether, Brandon Goodell and Aniket Kate. DL-SAG: Non-Interactive Refund Transactions For Interoperable Payment Channels in Monero. 24th International Conference on Financial Cryptography and Data Security (FC), Feb 2020. (22% acceptance rate)
- 49 Donghang Lu^{*G}, Tom Yurek, Samarath Kulshreshtha, Rahul Mahadev, Aniket Kate, and Andrew Miller. HoneyBadgerMPC and AsynchroMix: Practical Asynchronous MPC and its Application to Anonymous Communication. 26th ACM Conference on Computer and Communications Security (CCS), Nov 2019. (16% acceptance rate)
- 50 Duc V. Le^{*G}, Mahimna Kelkar^U, and Aniket Kate. Flexible Signatures: Towards Making Authentication Suitable for Real-Time Environments. European Symposium on Research in Computer Security (ESORICS), Sep 2019. (19% acceptance rate)
- 51 Michael Backes, Lucjan Hanzlik, Amir Herzberg, Aniket Kate, and Ivan Piryvalov^{*}. Efficient Non-Interactive Zero-Knowledge Proofs in Cross-Domains without Trusted Setup. 22nd International Conference on Practice and Theory of Public Key Cryptography (PKC), Apr 2019. (24% acceptance rate)
- 52 Giulio Malavolta^{*}, Pedro Moreno-Sanchez^{*G}, Clara Schneidewind, Aniket Kate, and Matteo Maffei. Anonymous Multi-hop Locks for Blockchain Scalability and Interoperability. Network and Distributed System Security Symposium (NDSS), Feb 2019 (17% acceptance rate)
- 53 Sze Yiu Chau^{*G}, Moosa Yahyazadeh, Omar Chowdhury, Aniket Kate, and Ninghui Li. Analyzing Semantic Correctness using Symbolic Execution: A Case Study on PKCS#1 v1.5 Signature Verification Network and Distributed System Security Symposium (NDSS), Feb 2019 (17% acceptance rate)
- 54 Sze Yiu Chau^{*G}, Bincheng Wang, Jianxiong Wang, Omar Chowdhury, Aniket Kate, and Ninghui Li. Why Johnny Can't Make Money With His Contents: Pitfalls of Designing and Implementing Content Delivery Apps. Annual Computer Security Applications Conference (ACSAC), pp. 236-251, December 2018. (20% acceptance rate)
- 55 Debajyoti Das^{*G}, Sebastian Meiser, Esfandiar Mohammadi, and Aniket Kate. Anonymity Trilemma: Strong Anonymity, Low Bandwidth, Low Latency—Choose Two. 39th IEEE Symposium on Security and Privacy (S&P (Oakland)), May 2018. (11% acceptance rate)

- 56 Pedro Moreno-Sanchez^{*G}, Navin Modi, Raghuvir Songhela, Aniket Kate, and Sonia Fahmy. Mind Your Credit: Assessing the Health of the Ripple Credit Network. 27th World Wide Web Conference (WWW), April 2018. (15% acceptance rate)
- 57 Stefanie Roos^{*}, Pedro Moreno-Sanchez^G, Aniket Kate, and Ian Goldberg. Settling Payments Fast and Private: Efficient Decentralized Routing for Path-Based Transactions.^M Network and Distributed System Security Symposium (NDSS), Feb 2018. (21% acceptance rate)
- 58 Giulio Malavolta^{*}, Pedro Moreno-Sanchez^{*G}, Aniket Kate, Matteo Maffei, and Srivatsan Ravi^P. Concurrency and Privacy with Payment-Channel Networks. 24th ACM Conference on Computer and Communications Security (CCS), Oct 2017 (18% acceptance rate)
- 59 David Chaum, Debajyoti Das^G, Farid Javani, Aniket Kate, Anna Krasnova, Joeri de Ruyter, & Alan T. Sherman. cMix: Mixing with Minimal Real-Time Asymmetric Cryptographic Operations. 15th International Conference on Applied Cryptography and Network Security (ACNS), Jun 2017 (23% acceptance rate)
- 60 Sze Yiu Chau^{*G}, Endadul Hoque, Omar Chowdhury, Huangyi Ge, Aniket Kate, Cristina Nita-Rotaru, and Ninghui Li. Systematically Finding Non-compliances In X.509 Certificate Validation Implementations. 38th IEEE Symposium on Security and Privacy (Oakland), May 2017 (13% acceptance rate)
- 61 Tim Ruffing^{*G}, Pedro Moreno-Sanchez^G, and Aniket Kate. P2P Mixing and Unlinkable Bitcoin Transactions. Network & Distributed System Security Symposium (NDSS), Feb 2017 (16% acceptance rate)
- 62 Giulio Malavolta^{*}, Pedro Moreno-Sanchez^{*G}, Aniket Kate, and Matteo Maffei. SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks. Network and Distributed System Security Symposium (NDSS), Feb 2017 (16% acceptance rate)
- 63 Michael Backes, Amir Herzberg, Aniket Kate, and Ivan Pryvalov^{*}. Anonymous RAM. 21st European Symposium on Research in Computer Security (ESORICS), Sep 2016 (21% acceptance rate)
- 64 Mainack Mondal^{*}, Johnatan Messias, Saptarshi Ghosh, Krishna P. Gummadi, and Aniket Kate. Forgetting in Social Media: Understanding and Controlling Longitudinal Exposure of Socially Shared Data. USENIX Symposium on Usable Privacy and Security (SOUPS), Jun 2016 (28% acceptance rate)
- 65 Bimal Viswanath^{*}, Muhammad Ahmad Bashir, Muhammad Bilal Zafar, Simon Bouget, Saikat Guha, Krishna P. Gummadi, Aniket Kate, and Alan Mislove. Strength in Numbers: Robust Tamper Detection in Crowd Computations. ACM Conference on Online Social Networks (COSN), Nov 2015 (27% acceptance rate)
- 66 Tim Ruffing^{*G}, Aniket Kate, and Dominique Schroeder. Liar, Liar, Coins on Fire!: Penalizing Equivocation By Loss of Bitcoins. 22nd ACM Conference on Computer and Communications Security (CCS), Oct 2015 (20% acceptance rate)
- 67 Satrajit Ghosh^G and Aniket Kate^{*}. Post-Quantum Forward Secure Onion Routing (Future Anonymity in Today's Budget). 13th International Conference on Applied Cryptography and Network Security (ACNS), Jun 2015 (21% acceptance rate)
- 68 Michael Backes, Aniket Kate, Sebastian Meiser^{*}, and Tim Ruffing^G. Secrecy without Perfect Randomness: Cryptography with (Bounded) Weak Sources. 13th International Conference on Applied Cryptography and Network Security (ACNS), Jun 2015 (21% acceptance rate)
- 69 Daniel Porto^{*}, Joao Leita0, Cheng Li, Allen Clement, Aniket Kate, Flavio Junqueira, and Rodrigo Rodrigues. Visigoth Fault Tolerance. European Conference on Computer Systems (EuroSys), Apr 2015 (21% acceptance rate)
- 70 Pedro Moreno-Sanchez^{*G}, Aniket Kate, Matteo Maffei, and Kim Pecina. Privacy Preserving Payments in Credit Networks. Network and Distributed System Security Symposium (NDSS), Feb 2015 (17% acceptance rate)
- 71 Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov^G. Privacy-preserving Data Aggregation with Optimal Utility. 30th Annual Computer Security Applications Conference (ACSAC), Dec 2014 (20% acceptance rate)
- 72 Michael Backes, Aniket Kate, Sebastian Meiser^{*}, and Esfandiar Mohammadi. (Nothing else) MATor(s): Monitoring the Anonymity of Tor's Path Selection. 21st ACM Conference on Computer and Communications Security (CCS), Nov 2014 (19% acceptance rate)

- 73 Tim Ruffing^{*G}, Pedro Moreno-Sanchez^G, and Aniket Kate. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. 19th European Symposium on Research in Computer Security (ESORICS), Sep 2014 (25% acceptance rate)
- 74 Michael Backes, Fabian Bendun, Ashish Choudhury, and Aniket Kate*. Asynchronous MPC with a Strict Honest Majority Using Non-equivocation. 33rd ACM Symposium on Principles of Distributed Computing (PODC), Jul 2014 (28% acceptance rate)
- 75 Michael Backes, Jeremy Clark, Peter Druschel, Aniket Kate, and Milivoj Simeonovski*. Introducing Accountability to Anonymity Networks. 12th International Conference on Applied Cryptography and Network Security (ACNS), Jun 2014 (22% acceptance rate)
- 76 Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi. AnoA: A Framework For Analyzing Anonymous Communication Protocols. 26th IEEE Computer Security Foundations Symposium (CSF), Jun 2013 (26% acceptance rate)
- 77 Michael Backes, Amit Datta^U, and Aniket Kate*. Asynchronous Computational VSS with Reduced Communication Complexity. Cryptographers' Track - RSA Conference (CT-RSA), Feb 2013 (28% acceptance rate)
- 78 Allen Clement, Flavio Junqueira, Aniket Kate*, and Rodrigo Rodrigues. On the (Limited) Power of Non-Equivocation. 31st ACM Symposium on Principles of Distributed Computing (PODC), Jul 2012 (26% acceptance rate)
- 79 Michael Backes, Ian Goldberg, Aniket Kate, and Esfandiar Mohammadi*. Provably Secure and Practical Onion Routing.^M 25th IEEE Computer Security Foundations Symposium (CSF), Jun 2012 (25% acceptance rate)
- 80 Michael Backes, Aniket Kate*, Matteo Maffei, and Kim Pecina. ObliviAd: Provably Secure and Practical Online Behavioral Advertising. 33rd IEEE Symposium on Security and Privacy (Oakland), May 2012 (13% acceptance rate)
- 81 Michael Backes, Ian Goldberg, Aniket Kate*, and Tomas Toft. Adding Query Privacy to Robust DHTs.^M 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS), May 2012 (22% acceptance rate)
- 82 Michael Backes, Aniket Kate, and Arpita Patra. Computational Verifiable Secret Sharing Revisited. 17th International Conference on the Theory and Application of Cryptology (ASIACRYPT), Dec 2011 (15% acceptance rate)
- 83 Aniket Kate*, Gregory M. Zaverucha, and Ian Goldberg. Constant-Size Commitments to Polynomials and Their Applications.^M 16th International Conference on the Theory and Application of Cryptology (ASIACRYPT), Dec 2010 (16% acceptance rate)
- 84 Aniket Kate* and Ian Goldberg. Distributed Private-Key Generators for Identity-Based Cryptography.^M 7th Conference on Security and Cryptography for Networks (SCN), Sep 2010 (28% acceptance rate)
- 85 Maxwell Young*, Aniket Kate, Ian Goldberg, and Martin Karsten. Practical Robust Communication in DHTs Tolerating a Byzantine Adversary.^M 30th International Conference on Distributed Computing Systems (ICDCS), Jun 2010 (14% acceptance rate)
- 86 Aniket Kate* and Ian Goldberg. Using Sphinx to Improve Onion Routing Circuit Construction.^M 14th International Conference on Financial Cryptography & Data Security (FC), Jan 2010 (19% acceptance rate)
- 87 Aniket Kate* and Ian Goldberg. Distributed Key Generation for the Internet.^M 29th International Conference on Distributed Computing Systems (ICDCS), Jun 2009 (16% acceptance rate)
- 88 Aniket Kate*, Gregory M. Zaverucha, and Urs Hengartner. Anonymity and Security in Delay Tolerant Networks. 3rd International Conf. on Security and Privacy in Communication Networks (SecureComm), Sep 2007 (26% acceptance rate)
- 89 Aniket Kate*, Gregory M. Zaverucha, and Ian Goldberg. Pairing-Based Onion Routing.^M 7th Privacy Enhancing Technologies Symposium (PET), Jun 2007 (19% acceptance rate).

REFEREED MAGAZINE ARTICLES

- 90 Ryan Henry, Amir Herzberg, and Aniket Kate. Blockchain Access Privacy: Challenges and Directions. IEEE Security and Privacy Magazine, July/August 2018.

- 91 Mainack Mondal*, Johnatan Messias, Saptarshi Ghosh, Krishna P. Gummadi, and Aniket Kate. Longitudinal Privacy Management in Social Media: The Need for Better Controls. *IEEE Internet Computing (IC)*, 21(3), 2017.

REFEREED WORKSHOP PAPERS

- 92 Easwar V Mangipudi*^G, Krutarth R Rao^U, Jeremy Clark, and Aniket Kate. Towards Automatically Penalizing Multimedia Breaches. *IEEE Security & Privacy on the Blockchain (IEEE S&B) Workshop*, Jun 2019.
- 93 Donghang Lu*^G, Pedro Moreno-Sanchez^G, Amanuel Zeryihun, Shivam Bajpayi^U, Sihao Yin^U, Ken Feldman, Jason Kosofsky, Pramita Mitra, and Aniket Kate. Reducing Automotive Counterfeiting using Blockchain: Benefits and Challenges. *IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, Apr 2019.
- 94 Adithya Bhat*^G, Pedro Moreno-Sanchez and Aniket Kate. Transitive Network: Tokenless IOU Credit Network in Ethereum. *Cryptocurrency Implementers' Workshop (CIW)*, co-located with FC 2019, Feb 2019.
- 95 Michael Backes, Niklas Grimm*^U, and Aniket Kate. Lime: Data Lineage in the Malicious Environment. *10th International Workshop on Security and Trust Management (STM)*, Sep 2014.
- 96 Tim Ruffing*^G, Jonas Schneider, Aniket Kate. Identity-Based Steganography and Its Applications to Censorship Resistance. *6th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)*, Jul 2013.
- 97 Michael Backes, Aniket Kate, and Esfandiar Mohammadi*. Ace: An Efficient Key-Exchange Protocol for Onion Routing. *11th ACM Workshop on Privacy in the Electronic Society (WPES)*, Oct 2012.

BOOKS AND BOOK CHAPTERS

- 98 Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov^G. Achieving Optimal Utility for Distributed Differential Privacy Using Secure Multiparty Computation. Book chapter, "Applications of Secure Multiparty Computation", *IOS CISS*, 13(5), 2015
- 99 Aniket Kate, Matteo Maffei, Giulio Malavolta, and Pedro Moreno-Sanchez^G. Credit Networks: Decentralized Designs and Privacy. To appear in *Morgan & Claypool's Information Security, Privacy, and Trust series*, pgs. 130, 2019

POSTERS

- 100 Tim Ruffing*^G, Jonas Schneider, Aniket Kate. Poster: Identity-based steganography and its applications to censorship resistance. *ACM Conference on Computer and Communications Security (CCS)*, Oct 2013
- 101 Michael Backes, Fabian Bendun, and Aniket Kate*. Brief Announcement: Distributed Cryptography using TrInc. *31st ACM Symposium on Principles of Distributed Computing (PODC)*, Jul 2012

THESES

- 102 Aniket Pundlik Kate: "Distributed Key Generation and Its Applications"
PhD Thesis, University of Waterloo, Jun 2010
- 103 Aniket Kate: "Frobenius Endomorphism Based Cryptosystems"
Master Thesis, Indian Institute of Technology–Bombay, Jun 2006

TECHNICAL REPORTS

- 104 Tiantian Gong*^G and Aniket Kate. Order but Not Execute in Order. *arXiv archive 2302.01177*, September 2023.
- 105 Sanjit Chatterjee, Deepak Garg, Aniket Kate*, and Tobias Theobald^G. Encrypting Messages for Incomplete Webs of Trust. *IACR Cryptology ePrint Archive 2017: 777*, August 2017.
- 106 Ivan Pryvalov*^G, Aniket Kate. Introducing Fault Tolerance into Threshold Password-Authenticated Key Exchange. *IACR Cryptology ePrint Archive 2014: 247*, July 2014.
- 107 Aniket Kate*, Yizhou Huang, and Ian Goldberg. Distributed Key Generation in the Wild.^M *IACR Cryptology ePrint Archive 2012/377*, Jul 2012.

SELECTED INVITED TALKS

NATIONAL AND INTERNATIONAL MEETINGS

- ◇ “Building Threshold Cryptosystems & MPC Applications over Blockchains Securely,” The Science of Blockchain Conference (SBC) 2024, NYC, USA. Aug 2024.
- ◇ “Mitigating Collusion in Secure Distributed Computing,” The 2024 Workshop on Competitive Economics of Cybersecurity, Sandia Labs/UNM, USA. May 2024.
- ◇ “Secure Allegation Escrows: Finding Safety in Numbers,” Re-Imagining Cryptography and Privacy (ReCAP) Workshop, USA. May 2024. (Virtual)
- ◇ “Building Threshold Cryptosystems & MPC Applications over Blockchains Securely,” D/Infra Summit, Denver, USA. Feb 2024.
- ◇ “Building Web3 Oracles,” Future Computing Research Workshop, Denver, USA. Feb 2024.
- ◇ “Building Threshold Cryptosystems & MPC Applications over Blockchains Securely,” Decentralized Physical Infrastructure (de:pin) Day, Denver, USA. Feb 2024.
- ◇ “Building Asynchronous Systems for a Simple Honest Majority Using a Chain of Integrity,” Science and Engineering of Consensus Workshop, Stanford University, USA. Aug 2023.
- ◇ “Distributed IOweYou Credit Networks,” Blockchain Kaigi, Japan. Jul 2022. (Virtual)
- ◇ “Cryptocurrencies, Blockchains, and NFTs,” All IN, Indiana NPR. Jan 2022.
- ◇ **Keynote:** “Rethinking Consensus for Fault-Tolerant CPS/IoT” at the Silicon Valley Cybersecurity Conference (SVCC). Dec 2021. (Virtual)
- ◇ “Crypto-economics by Combining Cryptography and Smart Contracts” at 2021 Dagstuhl seminar on Rigorous Methods for Smart Contracts. Oct 2021. (Virtual)
- ◇ “Reconfiguration Friendly Random Beacons,” Protocol lab Seminar Series. Oct 2021 (virtual).
- ◇ **Keynote:** “Blockchains + Network Privacy = A Nightmare” at the 9th International Workshop on Security in Blockchain and Cloud Computing (SBC). Jun 2021 (virtual).
- ◇ “Blockchains + Network Privacy = A Nightmare,” The 2020 Information Theory and Applications (ITA) Workshop, San Diego. Feb 2020.
- ◇ “Anonymous multi-hop locks for Blockchain scalability and interoperability,” Cryptoeconomic Systems Summit at the MIT Media Lab. Oct 2019.
- ◇ “Next Frontiers in Blockchains: Privacy and Interoperability,” Blockchain and Other Networks Conference, TTI/Vanguard, Washington, D.C. Sep 2019.
- ◇ “Blockchain Scalability and Interoperability,” Workshop on Security of Permissionless Systems (SPS), co-located with ACM PODC 2019. Aug 2019.
- ◇ **Keynote:** “Building Decentralized Credit Networks” at the Blockchain Connect Conference, San Francisco. Jan 2019.
- ◇ “Blockchain Contracts + Cryptography = Decentralized Economy!?” at the Workshop on Competitive Economics of Cybersecurity, Sandia National Laboratories. Nov 2018.
- ◇ “Inventing and Re-Inventing Blockchains for Supply-chain and IoT” at the 5th annual Indy Big Data Conferences. Sept 2018
- ◇ “Blockchain Privacy: Challenges, Solutions, and Unresolved Issues” at Blockchain and Cryptocurrency Workshop, Calgary, Canada. Aug 2017.
- ◇ **Keynote:** “Distributed IOweYou Credit Networks” at 18th International Conference on Distributed Computing and Networking (ICDCN), Hyderabad, India. Jan 2017.
- ◇ Tutorial: “An Introduction to Credit Networks” at ACM Conference on Computer and Communications Security (CCS), Vienna, Austria. Oct 2016.
- ◇ “Distributed IOweYou Credit Networks” at Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016), co-located with PODC 2016. July 2016.

- ◇ “(Working group) Genome Privacy: Architecture and middleware” at Dagstuhl Seminar 15431, Dagstuhl, Germany. Oct 2015.
- ◇ “Future Anonymity in Today’s Budget” at NIST Workshop on Cybersecurity in a Post-Quantum World (NIST PQC), Gaithersburg, USA. Apr 2015.
- ◇ “Asynchronous MPC with a Strict Honest Majority Using Non-equivocation” at Applied Multi-Party Computation Workshop, Microsoft Research, Redmond, USA. Feb 2014.
- ◇ “Anonymous Key Agreement in an Identity-based Infrastructure and its Applications” at the *MITACS 2009 Annual Conference*, Canada. Jun 2009.

UNIVERSITIES AND OTHER INSTITUTIONS

- ◇ “On-chain Randomness: Possibilities and Impossibilities,” IC3 Blockchain Camp 2024, Cornell Tech, NYC, USA. Jun 2024.
- ◇ “Building Asynchronous Systems for a Simple Honest Majority Using a Chain of Integrity,” Sky Seminar Series, University of California, Berkeley, USA. Aug 2023.
- ◇ “Advances in Privacy-Preserving Communication” at Distinguished Lecture Series (DLS) on Cyber Security and Privacy at IIT-Kharagpur, India. Oct 2021. (Virtual)
- ◇ “Designing and Analyzing Network Anonymity Solutions”, at Friedrich-Alexander-Universitaet Erlangen-Nuernberg (FAU), Germany, Jun 2021. (Virtual)
- ◇ Four lectures on “Blockchains and Cryptocurrencies” at UNAM/ITAM, Mexico City, Mar 2019.
- ◇ “Towards Inter-blockchain Communications”, Systems Seminar Speaker, Cornell University, Oct 2018.
- ◇ “Blockchains for (Digital) Supply Chains and Beyond”, Invited Speaker Series, SRC Inc, Syracuse, Oct 2018.
- ◇ “Blockchain Privacy : Challenges and Solutions” at the Workshop on Blockchain Technology, R C Bose Centre for Cryptology, Kolkata, India. Nov 2017. (Virtual Seminar)
- ◇ “Distributed IOweYou Credit Networks” at Visa Research, Palo Alto. Nov 2017.
- ◇ “Blockchain Privacy: Challenges, Solutions, and Unresolved Issues” at Cylab Distinguished Seminar Series, CMU. Oct 2017.
- ◇ Tutorial: “IOweYou Credit Networks” at 2nd Hebrew University Networking Summer, Jerusalem, Israel. Jun 2017.
- ◇ “IOweYou Credit Networks” at Information Trust Institute, University of Illinois at Urbana-Champaign, Mar 2017.
- ◇ “IOweYou Credit Networks” at CS, University of Wisconsin-Madison, Feb 2017.
- ◇ “Enabling trust with privacy in virtual marketplaces using credit networks” at Computer Science (CS) Colloquium Series, Indiana University, Bloomington. Apr 2016.
- ◇ “A little trusted hardware can go a long way towards privacy” at CASED, TU Darmstadt, Germany. Mar 2015.
- ◇ “Anonymous Communication Networks: Design, Analysis and Challenges” at TU Dresden, Germany. Sep 2014.
- ◇ “Differential Guarantees for Cryptographic Systems” at Microsoft Research, India. Apr 2014.
- ◇ “Towards Practical and Efficient Distributed Trust” at Indian Institute of Technology—Kharagpur (IIT-Kgp), India. Sep 2012.
- ◇ “An Interplay between Anonymity, Privacy, and Accountability” at *Indian Statistical Institute (ISI)*, India. Sep 2012.
- ◇ “Recent Improvements to Onion Routing” at *IBM Research - Zurich*, Rueschlikon, Switzerland. Jan 2012.
- ◇ “Recent Improvements in Onion Routing Circuit Construction” in the *Laboratory of Algorithmics, Cryptology and Security (LACS)*, University of Luxembourg, Luxembourg. Feb 2010.

OTHER PRESENTED PAPERS

- ◇ “Post-Quantum Forward-Secure Onion Routing - (Future Anonymity in Today’s Budget),” ACNS 2015, New York, Jun 2015.

- ◇ “Asynchronous MPC with a strict honest majority using non-equivocation,” ACM PODC 2014, Paris, July 2014.
- ◇ “Asynchronous Computational VSS with Reduced Communication Complexity,” CT-RSA 2013, San Francisco, Feb 2013
- ◇ “ObliviAd: Provably Secure and Practical Online Behavioral Advertising,” IEEE Symposium on Security and Privacy 2012, San Francisco, May 2012.
- ◇ “Adding query privacy to robust DHTs,” AsiaCCS 2012, Seoul, May 2012.
- ◇ “On the (limited) power of non-equivocation,” ACM PODC 2012, Mallorca, July 2012.
- ◇ “Constant-Size Commitments to Polynomials and Their Applications,” ASIACRYPT 2010, Singapore, Dec 2010.
- ◇ “Using Sphinx to Improve Onion Routing Circuit Construction,” Financial Cryptography 2010, Tenerife, Feb 2010.
- ◇ “Distributed Private-Key Generators for Identity-Based Cryptography,” SCN 2010, Amalfi, Sep 2010.
- ◇ “Distributed Key Generation for the Internet,” ICDCS 2009, Toronto, June 2009.
- ◇ “Anonymity and security in delay tolerant networks,” SecureComm 2007, Nice, September 2007.
- ◇ “Pairing-Based Onion Routing,” Privacy Enhancing Technologies 2007, Ottawa, July 2007.
- ◇ Talks and posters at workshops/events held at or by Purdue University, 2015-2020 (Selected):
 1. “Optimized Distributed Analytics for Dynamic CPS and IoT: Removing the Need for a Centralized Aggregator” 22nd Annual CERIAS Security Symposium, Purdue University, September 2020.
 2. “GDPR Privacy vs. Blockchain Transparency – Is it really technology against the law?” 21st Annual CERIAS Security Symposium, Purdue University, April 2019.
 3. “A Technical Perspective on the Future of Decentralization” 20th Annual CERIAS Security Symposium, Purdue University, April 2018.
 4. “Blockchains and Crypto Currencies From Hype to Reality Dawn or Doom” at Dawn-or-Doom 2017 Conference, Purdue University. Sep 2017

SOFTWARE SYSTEMS DEVELOPED

- ◇ “Code behind Tor Consensus Health project <https://consensus-health.torproject.org/>”, URL: <https://gitlab.torproject.org/zhtluo/depictor>. This library is built as a part of our IEEE S&P 2024 paper. This offers a reactive mechanism to detect any equivocation attack on Tor directory authorities.
- ◇ “OptRand — Optimistically Responsive Random Beacon”, URL: <https://github.com/libdist-rs/optrand-rs>. This rust library is built as a part of our NDSS 2023 paper: OptRand: Optimistically Responsive Reconfigurable Distributed Randomness. It offers a randomness beacon service to be used over the Internet.
- ◇ “Distributed Key Generation (DKG) for use over the Internet”, URL: <https://crysp.uwaterloo.ca/software/DKG/>. The DKG library is a multi-threaded C++ implementation associated with [55, 74]. It is employed and formed the basis of distributed key generation instantiations for distributed systems startups such as Helium, PoANetworks, and Tor.us.
- ◇ “Check Your Secondary Digital Footprint on Twitter!”, URL: <https://twitter-app.mpi-sws.org/footprint/>. This is an educational and informative Twitter app associated with [32] This app aims to educate users about their secondary digital footprints on systems such as Twitter and their risks.
- ◇ “DiceMix P2P mixing”, URL: <https://github.com/ElementsProject/dicemix>. This library is associated with [29]. The library is employed by privacy-preserving blockchains such as ElementsProject and Decred.

GRADUATED STUDENTS

GRADUATED PHD STUDENTS

- ◇ Tiantian Gong, Purdue University, Spring 2020–Fall 2024.
Thesis Title: Relax the Reliance on Honesty in Distributed Cryptographic Protocols.
Last known Employment: Post Doc, Yale/Technion
- ◇ Adithya Bhat, Purdue University, Fall 2018–Summer 2023.
Thesis Title: Pipelined Byzantine Fault Tolerance and Applications.
Last known Employment: Visa Research
- ◇ Donghang Lu, Purdue University, Fall 2017–Summer 2022.
Thesis Title: Efficient Building Blocks for Secure Multiparty Computation and Their Applications.
Last known Employment: TikTok
- ◇ Easwar V Mangipudi, Purdue University, Fall 2016–Summer 2022.
Thesis Title: Realizing information escrows and efficient key-management using threshold cryptography.
Last known Employment: Supra Oracles
- ◇ Debajyoti Das, Purdue University, Fall 2015–Summer 2021.
Thesis Title: Fundamental Constraints and Provable Secure Constructions for Anonymous Communication Protocol.
Last known Employment: Post Doc, KU Leuven, Belgium (on the faculty job market)
- ◇ Duc V Le (co-adviser: Mikhail Atallah) Purdue University, Fall 2016–Summer 2021.
Thesis Title: Efficient Cryptographic Constructions for Resource-Constrained Blockchain Clients,
Last known Employment: Visa Research
- ◇ Mohsen Minaei, Purdue University, Fall 2015–Summer 2020.
Thesis Title: Privacy-Preserving Systems with Crowd Blending
Last known Employment: Visa Research
- ◇ Sze Yiu Chau (co-advised with Ninghui Li), Fall 2015–Summer 2019.
Thesis title: Systematic Evaluation of Security Mechanism Deployments.
Last known Employment: Assistant Professor, Chinese University of Hong Kong (CUHK)
- ◇ Tim Ruffing, Saarland University (co-advised with Dominique Schroeder as I left Saarland), Spring 2013–Summer 2019.
Thesis title: Cryptography for Bitcoin and Friends.
Last known Employment: Blockstream
- ◇ Pedro Moreno-Sanchez, Purdue University, Fall 2013–Summer 2018.
Thesis title: Credit Network Payment Systems: Security, Privacy and Decentralization.
Last known Employment: Assistant Professor, IMDEA Software Institute, Madrid

GRADUATED MASTER THESIS STUDENTS

- ◇ Siddharth Gupta at Interdisciplinary Graduate Program in Information Security, CERIAS, 2016–2017.
Thesis title: Burning Bitcoins for Censorship Resistance.
- ◇ Simon Heinzl at Saarland University, Germany, 2015–2016.
Thesis title: Novel distributed trusted-party time-release encryption protocol.
- ◇ Tobias Theobald at Saarland University, Germany, 2015–2016.
Thesis title: Identity Web of Trust.
- ◇ Uzair Mahmood at Saarland University, Germany, 2014–2015.
Thesis title: Ensuring the Integrity of recommendations in a Marketplace.
- ◇ Ivan Pryvalov at Saarland University, Germany, 2013–2014.
Thesis title: Introducing Fault Tolerance into Threshold Password-Authenticated Key Exchange.

PREVIOUS POSTDOC

- ◇ Hai H. Nguyen, PostDoc in Computer Science.
Topic: Information Theoretic Cryptography. (Jan 2023-Aug 2023)
Last known Employment: ETH Zurich (PostDoc)

CURRENT STUDENTS

- ◇ Albert Yu, Ph.D. Student in Computer Sciences, (co-adviser: Hemanta Maji) Teaching Assistant.
Dissertation topic: Multi-party Computation. (Graduating in Summer 2025).
- ◇ Akhil S. Bandrupalli, Ph.D. Student in Computer Sciences, (co-adviser: Saurabh Bagchi) Research Assistant.
Dissertation topic: Consensus for CPS/IoT. (Prelim Exam planned in Fall 2024).
- ◇ Zhongtang Luo, Ph.D. Student in Computer Sciences, Research Assistant.
Dissertation topic: Distributed Systems: Attacks and Defenses. (Plan of Study is completed).
- ◇ Jianting Zhang, Ph.D. Student in Computer Sciences, Teaching Assistant.
Dissertation topic: Sharded Distributed Ledgers (Plan of Study in progress).
- ◇ Gustavo Franco Camilo, Ph.D. Student in Computer Sciences, Teaching Assistant.
- ◇ Satvinder Singh, Ph.D. Student in Computer Sciences, Research Assistant.

CURRENT POSTDOC

- ◇ Yanxue Jia, PostDoc in Computer Science.
Topic: Cryptography for Privacy Enhancing Technology. (Jan 2023-*present*)
(On academic job market 2024-25)

UNDERGRADUATE STUDENTS

- ◇ Sebastián Loza (supported by Purdue's Go Boiler program and grant money), 2024-25.
- ◇ Alejandra Gracia (supported by Purdue's Go Boiler program and grant money), 2024-25.
- ◇ Akshat Tej Neerati (supported by Undergraduate Research Fellowship, Purdue's Honors College), 2024-25.
- ◇ Shivam Bajpai (supported by Purdue SURF program and grant money), 2018–2019.
(Resulted Publication: [93])
- ◇ Sihao Yin (supported by Purdue's Summer Stay Scholar and grant money), 2018–2019.
(Resulted Publication: [93])
- ◇ Lizzy Tengana Hurtado (supported by Purdue's UREP-Columbia program and grant money), 2018.
(Resulted Publication: [8])
- ◇ Krutarth R. Rao (supported by Summer Stay Scholar and grant money), 2016–2018
(Resulted Publication: [2, 92])(**Received Outstanding Undergraduate Research Award, CS, Purdue, 2018**)
- ◇ Mahimna Kelkar (supported by NSF REU), 2016–2018.
(Resulted Publication: [50])
- ◇ Durga Keerthi Mandarapu (from IIT-Hyderabad) (supported by Purdue-CS GoBoiler program), 2018.
- ◇ Joy Wen (from U. Waterloo) (supported by Purdue-CS GoBoiler program), 2017.
- ◇ Rachit Garg (from IIT-Madras) (supported by Purdue Undergraduate Research Experience (PURE) program), 2016
- ◇ Niklas Grimm (Bachelor Thesis at Saarland University), 2012–2013.
(Resulted Publication: [14, 95])