Aditi Partap

aditi712@stanford.edu · https://aditi741997.github.io/ ·
https://github.com/aditi741997

Research Summary

My research focuses on applied cryptography, with a focus on designing accountable cryptographic protocols for decentralized systems. I work on threshold cryptographic primitives, such as signatures, secret sharing, encryption, and VRFs—which allow distributing trust among multiple parties to improve robustness. But traditionally, this comes at the cost of accountability. My work develops new definitions and constructions that achieve both decentralization and strong traceability guarantees against misbehaving parties: including accountable threshold signatures and decryption, traceable secret sharing for threshold as well as general access structures, and traceable threshold VRFs.

Education

Stanford University **September 2021 - Present**
Ph.D. in Computer Science *Advisor: Dan Boneh*
Cryptography

University of Illinois at Urbana-Champaign **August 2019 - May 2021**
M.S. in Computer Science *Advisors: Radhika Mittal & Brighten Godfrey*
Computer Networks & Systems

Indian Institute of Technology, Delhi **July 2014 - May 2018**
B.Tech. in Computer Science
CGPA: 9.675/10, Department Rank 1

Research Papers

Published

1. Dan Boneh, *Aditi Partap*, Lior Rotem. "Traceable Verifiable Random Functions" Accepted at the International Cryptology Conference (**Crypto 2025**) [eprint].

2. Dan Boneh, *Aditi Partap*, Brent Waters. "Accountable Multi-Signatures with Constant Size Public Keys" Accepted at Public Key Cryptography (**PKC 2025**) [eprint].

3. Dan Boneh, *Aditi Partap*, Lior Rotem. "Traceable Secret Sharing: Strong Security and Efficient Constructions" Accepted at the International Cryptology Conference (**Crypto 2024**) [eprint].

4. Dan Boneh, *Aditi Partap*, Lior Rotem. "Accountability for Misbehavior in Threshold Decryption via Threshold Traitor Tracing" Accepted at the International Cryptology Conference (**Crypto 2024**) [eprint].

5. Dan Boneh, *Aditi Partap*, Lior Rotem. "Proactive Refresh for Accountable Threshold Signatures" Accepted at Financial Cryptography and Data Security (**FC 2024**) [eprint].

6. Dan Boneh, *Aditi Partap*, Lior Rotem. "Post-Quantum Single Secret Leader Election (SSLE) From Publicly Re-randomizable Commitments" Accepted at Advances in Financial Technologies (**AFT 2023**) [eprint].

In submission

1. Vipul Goyal, Abhishek Jain, *Aditi Partap* "Traceable Secret Sharing Revisited" In submission at IACR EuroCrypt, 2026 [eprint]

2. Sourav Das, Pratish Datta, *Aditi Partap*, Swagata Sasmal, Mark Zhandry "Optimal Threshold Traitor Tracing" In submission at IACR EuroCrypt, 2026

3. Dan Boneh, Joachim Neu, Valeria Nikolaenko,, *Aditi Partap* "Data Availability Sampling with Efficient Repair: Definitions and New Constructions" In submission at IEEE S&P, 2025 [eprint]

Work Experience

Research Intern - NTT Research **Summer 2025**
Sunnyvale, CA

- Developed new definitions and constructions of secret sharing for general access structures, that also allows tracing misbehaving parties. Work submitted to EuroCrypt'26.
- Constructed the first threshold encryption schemes with traceability guarantees that achieve asymptotically optimal efficiency, i.e. the public key, ciphertext and secret keys scale only with log of the number of parties. Work submitted to EuroCrypt'26.

Research Intern - a16z Crypto **Summer 2024**
New York, NY

- Introduced the first framework for local repair in Data Availability Sampling (DAS) and constructed the first DAS scheme with efficient local repair, based on Multiplicity codes and a new polynomial commitment scheme. Work submitted to IEEE S&P'26.

Teaching

- Instructor for CS355: Advanced Cryptography, Spring 2024. Co-taught with Wilson Nguyen and Trisha Datta. [site]
- Undergraduate Teaching Assistant for Programming Languages course during Spring, 2018 and Data Structures & Algorithms course during Fall, 2017.

Service

- External reviewer for EuroCrypt 2025-26 and Crypto 2023-25, AsiaCrypt 2024-25 and Theory of Cryptography (TCC) 2024-25 conferences.
- Organizer of the Stanford Security Seminar from May, 2023 to current.
- Co-organizer of CS Graduate Women's Lunch at Stanford University.
- Designed a puzzle for ZK-Hacks III, based on the Cheon attack that can be used to break SNARK systems. Implemented a new BLS12 curve and the Cheon algorithm in arkworks.

Awards

- Stanford School of Engineering Graduate Fellowship. *2021*
- NSDI 2020 Diversity grant. *2020*
- Among Top 100 selected for Cornell, Maryland, Max Planck Pre-doctoral Research School (CMMRS). *2018*
- Institute Silver Medal for securing Department Rank 1 in Computer Science Dept. at IIT Delhi. *2018*
- All India Rank 7 in IIT Joint Entrance Examination (JEE Advanced) & secured 1st rank among girls. *2014*
- Among 16 students across all India to be awarded Aditya Birla Group Scholarship. *2014*
- All India Rank 208 among 1.4 million candidates appearing in JEE Mains organized in India by CBSE. *2014*
- Among Top 300 in Indian National Physics Olympiad. *2014*
- Among Top 30 in Indian National Mathematical Olympiad (INMO). *2013*
- Kishore Vaigyanik Protsahan Yojana Fellowship (KVPY) by Govt. of India. *2012-13*
- National Talent Search Examination (NTSE) scholarship (Top 1000 at National level). *2010*

Talks

"Data Availability Sampling with Repair"

1. University of Michigan, Ann Arbor Cryptography Seminar: November 2025

2. Science of Blockchain Conference (SBC): August 2025

"Traceable Verifiable Random Functions"

1. International Cryptography Conference (Crypto): August 2025
2. CIFRA Institute Cryptography Seminar (at Bocconi University): May 2025
3. EPFL Cryptography Seminar: May 2025
4. Cryptographic Tools for Blockchains Workshop (CTB): May 2025
5. Bay Area Cryptography Day: April 2025
6. University of California, San Diego Theory Seminar: April 2025
7. University of Washington, Seattle Cryptography Seminar: April 2025

"Accountable Multi-Signatures with Constant Size Public Keys"

1. Public Key Cryptography Conference (PKC): May 2025

"Traceable Secret Sharing: Strong Security and Efficient Constructions"

1. Conference on Information-Theoretic Cryptography (ITC): August 2025
2. University of California, Los Angeles Cryptography Seminar: April 2025
3. Bay Area Crypto Day: April 2024

"Accountability for Misbehavior in Threshold Decryption via Threshold Traitor Tracing"

1. International Cryptography Conference (Crypto): August 2024
2. New York University Cryptography Reading Group: June 2024
3. Carnegie Mellon University CyLab Cryptography Seminar: April 2024
4. NTT CIS Seminar: March 2024
5. University of California, Berkeley Security Seminar: November 2023
6. University of Maryland Cryptography Reading Group: October 2023

"Post-Quantum Single Secret Leader Election (SSLE) From Publicly Re-randomizable Commitments"

1. Advances in Financial Technologies (AFT): October 2023

"Proactive Refresh for Accountable Threshold Signatures"

1. Financial Cryptography (FC): March 2024
2. Microsoft Research Redmond Cryptography and Privacy Colloquium: June 2023
3. Brown University Cryptography Reading Group: May 2023
4. Stanford Security Workshop: April 2023
5. Bay Area Cryptography Day: April 2023

Past Research

1. Francisco Romero, Johann Hauswald, *Aditi Partap*, Daniel Kang, Matei Zaharia, Christos Kozyrakis "Optimizing video analytics with declarative model relationships" In Proceedings of the VLDB Endowment (VLDB), 2022.
2. *Aditi Partap*, Samuel Grayson, Muhammad Huzaifa, Sarita V. Adve, Brighten Godfrey, Saurabh Gupta, Kris Hauser, Radhika Mittal "On-Device CPU Scheduling for Sense-React Systems" In International Conference on Intelligent Robots and Systems (IROS), 2022.
3. Sachin Ashok, *Aditi Partap*, Ammar Tahir. "Fast and efficient lookups via data-driven FIB designs" In Proceedings of the ACM SIGCOMM Workshop on Future of Internet Routing Addressing (FIRA), 2022.
4. Danish Contractor, Krunal Shah, *Aditi Partap*, Parag Singla, Mausam. "Answering POI-recommendation Questions using Tourism Reviews" In Proceedings of the 30th ACM International Conference on Information Knowledge Management (CIKM), 2021.