# Aditi Partap

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

## 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*  *Advisor: 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

## INTERESTS & ONGOING RESEARCH

I'm broadly interested in applied cryptography, and am currently working on projects related to threshold signatures, threshold encryption and Post-quantum secure Single Secret Leader Election (SSLE).

## RESEARCH EXPERIENCE

**Accountable Multi-Signatures with Constant Size Public Keys**  **Summer'23 - Fall'23**
*Stanford University*  *Dan Boneh, Brent Waters*

- Constructed two new practical multisignatures which support local key generation, and have a constant size verifier key as well as signatures. Built two pairings-based constructions, one in the random oracle model, and one in the plain model.
- Constructed a pairings-based and a lattice-based multisignature which are more efficient but rely on a simple DKG protocol.
- In submission at EuroCrypt'24 (eprint)

**Traitor Tracing for Threshold Decryption**  **Summer'23 - Fall'23**
*Stanford University*  *Dan Boneh, Lior Rotem*

- Introduced the theory of accountability for threshold decryption by defining traitor tracing in the threshold setting.
- Constructed traitor tracing schemes for threshold decryption to trace a decoder from a greater-than-threshold quorum, to at least one traitor.
- Proved impossibility results for tracing a decoder from a below-threshold quorum. In this setting, we developed confirmation and tracing algorithms for a special class of decoders.
- In submission at EuroCrypt'24 (eprint)

**Post-Quantum Single Secret Leader Election (SSLE) From Publicly Re-randomizable Commitments**  **Fall'22 - Spring'23**
*Stanford University*  *Dan Boneh, Lior Rotem*

- Constructed the first efficient and plausibly post-quantum secure SSLE protocols based on LWE and Ring-LWE.
- Introduced publicly re-randomizable commitments (RRC), and constructed RRCs from lattices.
- Accepted at AFT'23 (eprint)

**Accountable Threshold Signatures with Proactive Refresh**                     **Summer'22 - Fall'22**
*Stanford University*                                                           *Dan Boneh, Lior Rotem*

- Introduced several definitions for proactive refresh (PR) for accountable threshold signatures (ATS), with different levels of security.
- Constructed practical ATS schemes with PR based on BLS and Schnorr signatures, that achieve unforgeability and weak accountability.
- Constructed generic ATS-PR schemes that achieve strong accountability.
- In submission at FC'24 (eprint)

**Memory Tagging: ARM MTE Pitfalls and Improvements**                           **Winter'22**
*Stanford Univerisity*                                                          *Dan Boneh*

- Surveyed how modern systems use ARM MTE for memory safety, and identified potential attacks in their designs.
- Developed & experimented with a memory efficient design for ARM MTE, which strengthens its security with minor performance overheads.
- In submission at AsiaCCS'23 (arXiv)

## ACTIVITIES & SERVICE

- 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.
- Co-chaired the Programmable networks session at HotNets'20.
- Undergraduate Teaching Assistant for Programming Languages course during Spring, 2018 and Data Structures & Algorithms course during Fall, 2017.

## 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*

## PAST RESEARCH EXPERIENCE

**DeepG2P: Fusing Multi-Modal Data to Improve Crop Production**                  **Summer'21**
*Microsoft Research*                                            *Ranveer Chandra & Anirudh Badam*

- Designed and developed a multi-modal neural network using convolution and attention mechanisms to predict agricultural yield based on seeds' DNA and environmental conditions of the farm.
- Trained and evaluated the model on Genome to Fields Maize dataset, and achieved 13-45% better prediction on unseen fields than existing methods.
- In submission at AISTATS'23 (arXiv)

**On-Device CPU Scheduling for Sense-React Systems**      **Fall'19 - Spring'21**
*University of Illinois at Urbana Champaign*      *Brighten Godfrey & Radhika Mittal*

- Developed a scheduling framework to manage compute resource allocation for sense - react systems, which dynamically adapts to variations in application requirements as well as available resources.
- Integrated the framework with ROS and ILLIXR (open source platforms for robotics and AR/VR) and improved performance for face tracking, robot navigation and VR applications.
- Accepted at IROS'22 (arXiv)

**Answering POI-recommendation Questions using Tourism Reviews**      **Fall'17 - Spring'18**
*Indian Institute of Technology, Delhi*      *Mausam & Parag Singla*

- Built an AI system that can answer multi faceted tourism questions from a huge set of answers.
- Applied a pipeline of NLP tools to extract correct entities from free text answers collected with online travel forum posts to curate a large 48k sized dataset.
- Designed & implemented a neural network employing LSTMs and attention mechanism & implemented a few OpenQA based research papers for baseline comparison.
- Accepted at CIKM'21 (arXiv).

## INDUSTRY EXPERIENCE

**Email Notification System for Power BI Service**      **December 2018 - August 2019**
*Microsoft Corporation, Vancouver, BC*

- Designed and implemented an email notification system which involved adding infrastructure support, efficiently querying the back-end database to identify users with expiring subscriptions, and extensive system testing.
- Developed various front-end features to improve customer engagement for the Power BI service.

**Deploying Tabular Data Models on Azure**      **May 2017 - July 2017**
*Microsoft Corporation, Redmond*

- Designed and developed a web application that allows users to deploy and visualize tabular models over their data on Azure Analysis Services.
- Used AngularJS framework to incorporate data binding and developed APIs in C# to connect to and fetch metadata from the user's database.
- Leveraged CRM solutions to integrate the app with Dynamics 365.

## SKILLS

Rust, Python, Java, C, C++, Git, LaTeX