Sai Rahul **Rachuri**

Research Scientist in Cryptography

385 Sherman Ave, Palo Alto, CA, 94085

pruners-treble.0g@icloud.com | rahulrachuri.github.io | RahulRachuri | Rahul Rachuri

Education

Visa Research — *California, USA*

Research Scientist — *Feb. 2023 - Present*

Aarhus University — *Aarhus, Denmark*

Post Doc. in Computer Science — *Dec. 2022 - Feb. 2023*

Aarhus University — *Aarhus, Denmark*

PhD in Computer Science — *Aug. 2019 - Nov. 2022*

- Thesis: Practical Multiparty Computation: Approaches to Private Machine Learning
- Advisors: Peter Scholl and Claudio Orlandi

International Institute of Information Technology, Bangalore (IIIT B) — *Bengaluru, India*

Integrated Master's (Bachelor's + Master's) in Information Technology — *Aug. 2014 - Jul. 2019*

- Thesis: Efficient Privacy-Preserving Machine Learning Using Mixed Multiparty Computation Protocols
- Advisor: Ashish Choudhury
- CGPA: 3.2/4

Narayana Junior College (Board of Intermediate Education) — *Hyderabad, India*

Higher Secondary Education (12th) — *Jun. 2012 - Mar. 2014*

- Percentage: 94.5%

Narayana Concept School (Board of Secondary Education) — *Hyderabad, India*

Secondary School Education (10th) — *Jun. 2011 - Mar. 2012*

- Grade Point: 9.3/10

Publications

Publications are listed in reverse chronological order.

1. Carsten Baum, Nikolas Melissaris, Rahul Rachuri, Peter Scholl. *Cheater Identification on a Budget: MPC with Identifiable Abort from Pairwise MACs*. *In Submission*. PDF
2. Lennart Braun, Mahak Pancholi, Rahul Rachuri, Mark Simkin. *Ramen: Souper Fast Three-Party Computation for RAM Programs*. *In Submission*. PDF
3. Rahul Rachuri, Peter Scholl. *Le Mans: Dynamic and Fluid MPC for Dishonest Majority*. *CRYPTO 2022*. PDF
4. Nishat Koti, Arpita Patra, Rahul Rachuri, Ajith Suresh. *Tetrad: Actively Secure 4PC for Secure Training and Inference*. *NDSS 2022*. PDF
5. Daniel Escudero, Satrajit Ghosh, Marcel Keller, Rahul Rachuri, and Peter Scholl. *Improved Primitives for MPC over Mixed Arithmetic-Binary Circuits*. *CRYPTO 2020*. PDF
6. Rahul Rachuri, Ajith Suresh. *Trident: Efficient 4PC Framework for Privacy Preserving Machine Learning*. *NDSS 2020*. PDF
7. Seetarama Raju Pericherla, Rahul Rachuri, Shrisha Rao. *Modeling Confirmation Bias Through Egotism and Trust in a Multi Agent System*. *IEEE SMC 2018*. PDF

Workshops/Posters

1. Rahul Rachuri, Peter Scholl. *Le Mans: Dynamic and Fluid MPC for Dishonest Majority*. *To Appear at Theory and Practice of Multi-Party Computation Workshop 2022*. PDF
2. Nishat Koti, Arpita Patra, Rahul Rachuri and Ajith Suresh. *Tetrad: Actively Secure 4PC for Secure Training and Inference*. *PPML 2021 at ACM CCS*. PDF

3. Daniel Escudero, Matthew Jagielski, Rahul Rachuri, Peter Scholl. *Adversarial Attacks and Countermeasures on Private Training in MPC*. *PPML-NeurIPS 2020*. PDF
4. Daniel Escudero, Satrajit Ghosh, Marcel Keller, Rahul Rachuri, and Peter Scholl. *Improved Primitives for MPC over Mixed Arithmetic-Binary Circuits*. *Theory and Practice of Multi-Party Computation Workshop 2020*. PDF

Talks and Presentations

1. January 2022. *Le Mans: Dynamic and Fluid MPC for Dishonest Majority*. Colloquium Seminar @ BIU.
2. September 2021. *Secure Machine Learning with Multiparty Computation*. DIREC Seminar.
3. December 2020. *Adversarial Attacks and Countermeasures on Private Training in MPC*. PPML-NeurIPS 2020.
4. August 2020. *Improved Primitives for MPC over Mixed Arithmetic-Binary Circuits*. CRYPTO 2020.
5. June 2020. *Improved Primitives for MPC over Mixed Arithmetic-Binary Circuits*. Theory and Practice of Multi-Party Computation Workshops.

Professional Activities

As an external reviewer:

2023	ACNS, TDSC, ITC, PETS
2022	PETS, Eurocrypt, CANS, Asiacrypt
2021	Eurocrypt, ACISP, PETS
2020	CRYPTO, ACM CCS, Asiacrypt

Conference and Workshop Participation

2022	TPMPC, Bar-Ilan Winter School
2021	Crypto (virtual), Eurocrypt, DIREC workshop
2020	Crypto (virtual), Eurocrypt (virtual), TPMPC (virtual), ACM CCS (virtual), PPML-NeurIPS (virtual)
2019	ACM CCS

Research Experience

Center for Research in Applied Cryptography and Cyber Security, Bar-Ilan University — *Ramat Gan, Israel*
Visiting Researcher — *Oct. 2021 - Feb. 2022*
- Host: Benny Pinkas

Cryptography and Information Security Lab, Indian Institute of Science — *Bengaluru, India*
Visiting Researcher — *Oct. 2018 - Jun. 2019*
- Host: Arpita Patra

Center for Research in Applied Cryptography and Cyber Security, Bar-Ilan University — *Ramat Gan, Israel*
Research Intern — *Jun. 2018 - Jul. 2018*
- Program: International Summer Program/Internship in Applied MPC and Implementations

Teaching Experience

Aarhus University — *Aarhus, Denmark*
Computability and Logic (Bachelor) — *Spring 2021*

Aarhus University — *Aarhus, Denmark*
Computability and Logic (Bachelor) — *Spring 2020*

Aarhus University — *Aarhus, Denmark*
Cryptology (Master) — *Fall 2019*

Aarhus University *Aarhus, Denmark*

Machine Learning (Bachelor) *Fall 2019*

International Institute of Information Technology, Bangalore *Bengaluru, India*

Foundations of Cryptography (Bachelor) *Fall 2018*

International Institute of Information Technology, Bangalore *Bengaluru, India*

Introduction to Automata Theory and Computability (Bachelor) *Spring 2018*

Projects

IIIT Bangalore *Bengaluru, India*

IP Management System Portal *Oct. 2016 - Dec. 2016*

- Course: Database Systems
- An intra-college Intellectual Property Management System, which efficiently manages patent, licensing and royalty claims for projects and products worked on by members of the university. A web app was designed with different views for different users, such as Student, Faculty, IP Committee or a Guest.
- Tools used: Ruby on Rails, MySQL, HTML, CSS

IIIT Bangalore *Bengaluru, India*

LED Matrix Display *Mar. 2015 - Apr. 2015*

- Course: Basic Electronics
- Built a 24x6 LED matrix display controlled by an Arduino which displays scrolling text based on the input given.
- Tools used: Arduino, LEDs, soldering equipment

IIIT Bangalore *Bengaluru, India*

Battleship *Nov. 2014 - Dec. 2014*

- Course: C Programming
- Built a game of battleship in C, where the player plays against the computer. The computer had a strategy built into it that analyses the output of its previous move to decide the next one.

Skills

Programming C/C++, Python, Java, LaTeX

DevOps Docker

Languages English, Telugu, Hindi