

# Sai Rahul Rachuri

PHD STUDENT

Nygaard 286, Department of Computer Science, Åbogade 34, 8200 Aarhus, Denmark

+45 31 86 34 17 | [rachuri@cs.au.dk](mailto:rachuri@cs.au.dk) | [rahulrachuri.github.io](https://github.com/rahulrachuri) | [RahulRachuri](https://www.linkedin.com/company/rahulrachuri) | [Rahul Rachuri](https://www.linkedin.com/company/rahulrachuri) | [@iamRachuri](https://twitter.com/iamRachuri)

## Education

### Aarhus University

PHD IN COMPUTER SCIENCE

- Area: Privacy-Preserving Technologies
- Advisors: [Peter Scholl](#) and [Claudio Orlandi](#)

Aarhus, Denmark

Aug. 2019 - Present

### International Institute of Information Technology, Bangalore (IIIT B)

INTEGRATED MASTER'S (BACHELOR'S + MASTER'S) IN INFORMATION TECHNOLOGY

- Specialisation: Secure Multiparty Computation (MPC)
- Thesis Title: Efficient Privacy-Preserving Machine Learning Using Mixed Multiparty Computation Protocols
- Advisor: [Ashish Choudhury](#)
- CGPA: 3.2/4

Bengaluru, India

Aug. 2014 - Jul. 2019

### Narayana Junior College (Board of Intermediate Education)

HIGHER SECONDARY EDUCATION (12TH)

- Percentage: 94.5%

Hyderabad, India

Jun. 2012 - Mar. 2014

### Narayana Concept School (Board of Secondary Education)

SECONDARY SCHOOL EDUCATION (10TH)

- Grade Point: 9.3/10

Hyderabad, India

Jun. 2011 - Mar. 2012

## Publications

Publications are listed in reverse chronological order.

- Rahul Rachuri, Peter Scholl. *Le Mans: Dynamic and Fluid MPC for Dishonest Majority*. CRYPTO 2022. [PDF](#)
- Nishat Koti, Arpita Patra, Rahul Rachuri, Ajith Suresh. *Tetrad: Actively Secure 4PC for Secure Training and Inference*. NDSS 2022. [PDF](#)
- Daniel Escudero, Satrajit Ghosh, Marcel Keller, Rahul Rachuri, and Peter Scholl. *Improved Primitives for MPC over Mixed Arithmetic-Binary Circuits*. CRYPTO 2020. [PDF](#)
- Rahul Rachuri, Ajith Suresh. *Trident: Efficient 4PC Framework for Privacy Preserving Machine Learning*. NDSS 2020. [PDF](#)
- 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

- 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](#)
- Nishat Koti, Arpita Patra, Rahul Rachuri and Ajith Suresh. *Tetrad: Actively Secure 4PC for Secure Training and Inference*. PPML 2021 at ACM CCS. [PDF](#)
- Daniel Escudero, Matthew Jagielski, Rahul Rachuri, Peter Scholl. *Adversarial Attacks and Countermeasures on Private Training in MPC*. PPML-NeurIPS 2020. [PDF](#)
- 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

- January 2022. *Le Mans: Dynamic and Fluid MPC for Dishonest Majority*. Colloquium Seminar @ BIU.
- September 2021. *Secure Machine Learning with Multiparty Computation*. DIREC Seminar.
- 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
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

VISITING RESEARCHER

- Host: Benny Pinkas

*Ramat Gan, Israel*

*Oct. 2021 - Feb. 2022*

### Cryptography and Information Security Lab, Indian Institute of Science

VISITING RESEARCHER

- Host: Arpita Patra

*Bengaluru, India*

*Oct. 2018 - Jun. 2019*

### Center for Research in Applied Cryptography and Cyber Security, Bar-Ilan University

RESEARCH INTERN

- Program: International Summer Program/Internship in Applied MPC and Implementations

*Ramat Gan, Israel*

*Jun. 2018 - Jul. 2018*

## Teaching Experience

---

### Aarhus University

COMPUTABILITY AND LOGIC (BACHELOR)

*Aarhus, Denmark*

*Spring 2021*

### Aarhus University

COMPUTABILITY AND LOGIC (BACHELOR)

*Aarhus, Denmark*

*Spring 2020*

### Aarhus University

CRYPTOLOGY (MASTER)

*Aarhus, Denmark*

*Fall 2019*

### Aarhus University

MACHINE LEARNING (BACHELOR)

*Aarhus, Denmark*

*Fall 2019*

### International Institute of Information Technology, Bangalore

FOUNDATIONS OF CRYPTOGRAPHY (BACHELOR)

*Bengaluru, India*

*Fall 2018*

### International Institute of Information Technology, Bangalore

INTRODUCTION TO AUTOMATA THEORY AND COMPUTABILITY (BACHELOR)

*Bengaluru, India*

*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