Utkarsh Parkhi

https://utkarshparkhi.github.io NYC, New York, USA +1 (201)-275-8337

Education

New York University, Courant, September 2023-May 2025
Master of Science in Computer Science GPA: 3.9/4.0 NYC, New York, USA
Thesis: Fine Grained Cryptography Advisor: Dr Marshall Ball

Indian Institute of Technology, Roorkee, September 2018-May 2022
Bachelor of Technology in Engineering Physics GPA: 7.2/10 Roorkee, UK, India

Research Interests

- Complexity Theory
- Foundations of Cryptography
- Meta-Complexity
- Hardness Magnification
- Zero Knowledge Proofs

Research Experience

Accumulation without Homomorphism with Dr. Bennedikt Bünz September 2024-Present

- Reviewing relevant literature to support development and optimization of the Accumulation scheme
- Developing the accumulation scheme using quantum-secure Merkle trees and error-correcting codes.

Fine Grained Cryptography with Dr. Marshall Ball Jan 2024-Present

Work in the intersection of Cryptography and Complexity Theory

- Investigated the problems in Fine Grained Cryptography came up with black box separations for existence of Fine Grained One Way Functions from $P \neq NP$ assumption.
- Further examined the Fine Grained analogues of Cryptographic Primitives like OWF, PRG, PRF and attempted to Magnify the respective hardness properties.
- Studied the existing Hardness Magnification/Amplification phenomenon in Meta-Complexity and Self Reducibility of some specific Problems

ZK-friendly Hash Function with Dr. Bennedikt Bünz Summer 2024

Worked on zk-friendly hash functions.

- Implemented the *Monolith permutation and a generic Sponge framework using Arkworks in rust.*
- *Designed the constraints for monolith in R1CS so that it can be used in already popular groth based proof systems*
- *Achieved native performance of* $4.34\mu s$ *for sponge based compression and* $1.79\mu s$ *for 2-to-1 compression*

Timetabler with IMG, IIT Roorkee Spring 2021

Worked on automating the system for scheduling lectures for a semester at University

- Formulated timetable constraints as a Satisfiability (SAT) problem, covering course requirements, instructor availability, and room capacities.
- Developed and implemented a scheduling engine to automate university timetable creation, enhancing efficiency and accuracy.

Machine Learning in Scintillation Detectors with Dr Anil Kumar Gourishetty Fall 2021

Worked on leveraging Machine Learning for Scintillation Detectors

- Evaluated multiple ML models for pulse shape discrimination in scintillation detectors to enhance radiation detection
- Achieved 99.71% accuracy using ANN, outperforming Logistic Regression and SVM

Coursework Projects

CSCI-GA.3033 Cryptography of Blockchains with Dr. Bennedikt Bünz Spring 2024

- Partnered with fellow students and worked on implementing ZCash framework.
- Utilized Arkworks, a Rust-based library for zk-SNARKs, to implement the Spend and Output circuits of the Zero Cash framework.
- Optimized the framework by reducing the number of constraints by approximately 40,000 through the integration of the Poseidon hash function, replacing the previously used Blake hash.

Industry Experience

Flipkart June 2022 - July 2023

Software Developer

- Created 2 new carousels on the search page, which boosted ad revenue by 6 million USD
- Performed a meticulous legacy code audit, leading to a 4,000-line reduction, thereby enhancing efficiency and maintainability
- Restructured backend cron jobs and Airflow DAGs while migrating to GCP clusters

Flipkart June 2021 - August 2021

Software Developer Intern

- Implemented a web scraper for third-party mobile reviews using Scrapy and Beautiful Soup.
- Utilized Facebook BART NLP models for extracting concise summaries from online reviews
- Leveraged the RoBERTa sentiment analysis model to assess and rate these reviews effectively
- Technology Used: JAVA, Python, Scrapy, Beautiful Soup, Hugging Face, Kubernetes, Docker, Google Cloud Platform,

Relevant Coursework

Honors Analysis of Algorithms, Geometric Methods in Algorithm Design, Introduction to Graduate Cryptography, Quantum Computing, Cryptography of Blockchains, Discrete Mathematics, Cryptography of Blockchains, Programming Languages, Operating Systems, Optimization Techniques

Teaching Experience

NYU CSCI-GA.3520 Honors Analysis of Algorithms *Course Assistant* Fall 2024
NYU CS-GY 6043 Design and Analysis of Algorithms II *Grading Assistant* Fall 2024
NYU CSCI-GA.3210-001 Introduction To Cryptography *Grading Assistant* Fall 2024
NYU CSCI-UA.0310-001 Basic Algorithms, *Tutoring Assistant* Summer 2024
NYU CSCI-UA.0310-007 Basic Algorithms, *Grading Assistant* Spring 2024

Awards

ICPC Greater New York Regionals, Team Rank 26 (Second best team at NYU)

Community Involvement

NYU Theory Seminar, 2023-2025
National Social Service, Volunteer teaching high school students 2018
Programming and Algorithms Group, IIT Roorkee
Information Management Group, IIT Roorkee
SPICMACAY, *Volunteer* 2018

References

Dr. Marshall Ball
Assistant Professor of Computer Science at NYU, Courant

Dr. Bennedikt Bünz
Assistant Professor of Computer Science at NYU Courant,

Dr. Anil K Gourishetty
Professor of Physics at IIT Roorkee,