ADITYA GULATI

github.com/ditttu adityagulatiadityagulati@gmail.com adityagulati@ucsb.edu

RESEARCH INTERESTS

Psuedorandom Quantum States (PRS), Quantum Cryptography, Post-Quantum Cryptography

EDUCATION

University of California Santa Barbara *2022 - Present*
Ph.D., Computer Science, GPA - 4.00
Chancellor Fellowship
Advisor - Prabhanjan Ananth
Topic - Quantum Cryptography

Indian Institute of Technology, Kanpur *2017 - 2021*
B.S., Mathematics and Scientific Computing.
Minor in Theory of Computation
Minor in Algorithms
Minor in Linguistics

PUBLICATIONS AND PREPRINTS

Pseudorandom Quantum States, Revisited: New Properties, Variants, Constructions and Cryptographic Applications
Prabhanjan Ananth, Aditya Gulati, Louwen Qian, Henry Yuen.
Quantum Information Processing (QIP), 2023 (Short plenary talk)

Pseudorandom (Function-Like) Quantum State Generators: New Definitions and Applications
Prabhanjan Ananth, Aditya Gulati, Louwen Qian, Henry Yuen.
Theory of Cryptography Conference (TCC), 2022
Quantum cryptography conference (QCRYPT), 2022

On algorithms to find p-ordering
Aditya Gulati, Sayak Chakrabarti, Rajat Mittal.
7th Annual International Conference on Algorithms and Discrete Applied Mathematics (CALDAM), 2021.

Accelerating 2PC-based ML with Limited Trusted Hardware
Muqsit Nawaz, Aditya Gulati, Kunlong Liu, Vishwajeet Agrawal, Prabhanjan Ananth, Trinabh Gupta.
arXiv:2009.05566 (Pre-print).

RESEARCH EXPERIENCE

Designing Quantum Cryptography Protocols *August 2020 - June 2022*
Advisor: Prof. Prabhanjan Ananth (UCSB)
Designed and constructed quantum cryptography protocols for psuedorandom quantum states, secure multiparty computation and indistinguishability obfuscation.

Analysis of properties of polynomials over $\mathbb{Z}/p^k\mathbb{Z}$ *January 2019 - March 2021*
Advisor: Prof. Rajat Mittal (IIT Kanpur)
Worked on a theory of root-sets for polynomials over $\mathbb{Z}/p^k\mathbb{Z}$. Analysed the properties of root-sets using p-orderings.

Investigation and implementation of Secure 2-party protocols for private ML *January 2020 - July 2020*
Advisor: Prof. Trinabh Gupta (UCSB)
Studied and implemented various 2 party schemes to create a private ML system. Created optimisations on existing implementation of various 2 party schemes.

Analysis of Core for Three Player Cooperative Games *January 2021 - May 2021*
Advisor: Prof. Amit Kuber (IIT Kanpur)
Analysed the core stability and core non-emptiness problem for three player cooperative games. Came up with a set of constant time checkable conditions for stability and non-emptiness.

WORK EXPERIENCE

Helper4U *Feb 2021 - July 2021*

Security Intern

Worked on a php backend to secure APIs and test for vulnerabilities. Load-tested the backend and posted to a scalable build using dockers.

New York Office, IIT Kanpur *May 2018 - August 2018*

Backend Development Intern

Worked on a scalable microservice based web application with an extensive technology stack of Scala, Slick, PostgreSQL, Couchbase, Kafka etc.

TEACHING EXPERIENCE

Randomized Methods in Computation Complexity *Summer 2021*

Project Mentor, Dept. of Computer Science (IIT Kanpur)

Mentored a group of 10 juniors in various randomized methods in computation complexity. Took lectures on Polynomial Identity Testing, Expanders, Pseudorandom Generators, Error Correcting Codes and Hardness vs Randomness.

Fully Homomorphic Encryption and Functional Secret Sharing *Summer 2019*

Project Mentor, Dept. of Computer Science (IIT Kanpur)

Lead a group of 4 students to read and implement papers on FHE and FSS. Used GPU to parallelise the encryption algorithm and gain a 50x faster running speed.

Cryptanalysis of Block Ciphers *Fall 2019*

Project Mentor, Dept. of Mathematics (IIT Kanpur)

Mentored a group of 15 sophomores to implement, analyse and attack weaker versions of AES and DES. Introduced them to attack models and various known attacks.

ESC101A: Fundamentals of Computing *Fall 2018*

Academic Mentor, Dept. of Computer Science (IIT Kanpur)

Mentored a group of 30 freshmen for the fundamentals of computing course. Designed assignments and conducted doubt clearing sessions for the same. Took extra lectures for supplementary topics not covered by the instructor.

SKILLS

Languages: Python, C++, Rust, Bash, Haskell.
Software & Tools: Git, Sage, Numpy, Sympy, matplotlib.

AWARDS AND ACHIEVEMENTS

- **Chancellor Fellowship UCSB**, recipient of the prestigious Chancellor Fellowship at UCSB. - **Springer Best Student Paper Presentation Award**, 7th Annual International Conference on Algorithms and Discrete Applied Mathematics (CALDAM), 2021.
- **KVPY Fellow**, Department of Science and Technology, Government Of India.
- **Secured the rank - 639**, in JEE Advanced 2017 among 1.2 million students.

RELEVANT COURSES

Relevant Computer Science Courses

ESC101 - Fundamentals of Computing	CS641 - Modern Cryptography
ESO207 - Data Structures & Algorithms	CS682 - Quantum Computing
CS340 - Theory of Computation	CS345 - Algorithms II
EE667 - Information Theory	CS648 - Randomised Algorithms
CS747 - Randomized Methods in Computational Complexity	CMPSC 211A - Matrix Analysis and Computation
CMPSC 291K - Special Topics in Deep Learning	CMPSC 271A - Advanced Distributed Systems

Relevant Mathematics Courses

MTH102 - Linear Algebra	MTH201 - Linear Algebra II
MTH204 - Abstract Algebra	MTH302 - Set Theory & Logic
MSO201 - Probability & Statistics	MTH701 - Modal Logic
MTH712 - Algebraic Number Theory	MTH678 - Combinatorics