ADITYA GULATI

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

RESEARCH INTERESTS

Psuedorandom Quantum States (PRS) and Microcrypt, Quantum Cryptography, Quantum Circuit Synthesis and Optimization, Quantum Computational Complexity

EDUCATION

University of California Santa Barbara *2022 - Present*
Ph.D., Computer Science, GPA - 3.95
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

Cryptography in the Common Haar State Model: Feasibility Results and Separations
Prabhanjan Ananth, Aditya Gulati, Yao-Ting Lin.
QCRYPT 2024, TCC 2024

Pseudorandom Isometries
Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, Yao-Ting Lin.
Eurocrypt 2024

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

Study in Quantum Pseudorandomness *June 2024 - August 2024*
Advisor: Prof. Kai-Min Chung (Academia Sinica, Taipei)
Conducted research under Prof. Kai-Min Chung, focusing on state testing, quantum languages, and pseudorandomness in quantum cryptography.

Designing Quantum Cryptography Protocols *August 2020 - Present*
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.

CONFERENCE REVIEWS

Conferences: PKC’22, CRYPTO’22, EUROCRYPT’23, ITC’23, QIP‘24, STACS‘24, TQC‘24, CRYPTO‘24

TEACHING EXPERIENCE

Teaching Assistant, Automata Theory *Spring 2023, Fall 2023*
Department of Computer Science (UCSB)
Supported the instructor in conducting review sessions, grading assignments, and providing individualized guidance. My role included fostering collaborative learning environments and contributing to the development of instructional materials to enhance the overall learning experience for students.

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.

SKILLS

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

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

CMPSC 292G - Topics in Quantum Cryptography CS641 - Modern Cryptography
ESO207 - Data Structures & Algorithms CS682 - Quantum Computing
CMPSC 293G - Topics in Quantum Systems Design CMPSC 292F - Graph Neural Networks
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 MTH102 - Linear Algebra
MTH201 - Linear Algebra II
MTH204 - Abstract Algebra MSO201 - Probability & Statistics