

# RISHABH RANJAN

☎ 858-405-1419 ✉ [riranjan@ucsd.edu](mailto:riranjan@ucsd.edu) [in linkedin.com/in/ranjan-rishabh](https://www.linkedin.com/in/ranjan-rishabh) [github.com/ranjan-rishabh](https://github.com/ranjan-rishabh)

## Education

|                                                                                                                                |                                          |
|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <b>University of California, San Diego</b><br><i>Doctor of Philosophy in Computer Science (Advised by Prof. Mihir Bellare)</i> | <b>Sep. 2021 – June 2026</b><br>3.97/4.0 |
| <b>University of California, San Diego</b><br><i>Masters of Science in Computer Science</i>                                    | <b>Sep. 2021 – June 2023</b><br>3.97/4.0 |
| <b>Birla Institute of Technology, Mesra</b><br><i>Bachelors of Engineering in Computer Science and Engineering</i>             | <b>July 2015 – June 2019</b><br>8.41/10  |

## Experience

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| <b>Seagate Technology</b><br><i>Cryptography Research Intern</i> <ul style="list-style-type: none"><li>Developed and analysed security of secure computation protocol based on Fully Homomorphic Encryption and Zero-Knowledge Proofs.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>June 2024 – Sept 2024</b><br><i>Shakopee, MN</i>     |
| <b>Microsoft</b><br><i>Software Engineer</i> <ul style="list-style-type: none"><li>Designed and developed features for multiple Azure extensions as part of the Azure Storage team.</li><li>Owner of multiple areas such as 'ordering' and 'virtual machines' in the Azure Stack Edge extension.</li><li>Founding developer of the new Edge Ordering extension. Now generally available and being used by multiple teams in Azure and beyond.</li><li>Automated deployment of microservices to ServiceFabric clusters saving developer time in each release cycle.</li><li>Technologies: <i>Node, Typescript/JavaScript, C#, ReactJS, KnockoutJS, Redux</i></li></ul> | <b>July 2019 – Sep. 2021</b><br><i>Bangalore, India</i> |
| <b>Microsoft</b><br><i>Software Engineering Intern</i> <ul style="list-style-type: none"><li>Created a Visual Studio extension based on syntax parsing and compilation to provide real time warnings about accessibility violations in code. Received Pre-Placement Offer for this.</li><li>Alleviated the need for accessibility testing as a stage in development and saved hundreds of developer hours.</li><li>Technologies: <i>C#, Managed Extensibility Framework, Roslyn (compiler platform for Visual Studio)</i></li></ul>                                                                                                                                   | <b>May 2018 – July 2018</b><br><i>Hyderabad, India</i>  |

## Publications

- Mihir Bellare, Rishabh Ranjan, Doreen Riepel, Ali Aldakheel (2024), *The Concrete Security of Two-Party Computation: Simple Definitions, and Tight Proofs for PSI and OPRFs*, **Asiacrypt 2024**.
- Paarth Neekhara, Shehzeen Hussain, Rafael Valle, Boris Ginsburg, Rishabh Ranjan, Shlomo Dubnov, Farinaz Koushanfar, Julian McAuley, *SelfVC: Voice Conversion With Iterative Refinement using Self Transformations*, **ICML 2024**.
- Rishabh Ranjan, Dr. Vathsala H, Dr Shashidhar G Koolagudi (2021), *Profile Generation from Web Sources: An Information Extraction System*, **Soc. Netw. Anal. Min. (Springer) 12, 2 (2022)**.

## Technical Skills

**Languages:** C, C++, Python, TypeScript, C#, SQL  
**Frameworks:** OpenFHE, Tensorflow, PyTorch, MPI  
**Areas:** Provable security, Multi-party computation, Post-quantum cryptography

## Relevant Graduate Courses

**Cryptography :** Lattice Algorithms, Modern Cryptography, Applied Cryptography, Advanced Cryptography (FHE), Quantum Cryptography  
**Complexity theory :** Computability and Complexity, Analysis of Algorithms, Semi-definite Programming  
**Systems :** Advanced Compiler Design, Parallel and Distributed Computing

## Projects

---

### Verifiable Homomorphic Encryption using CF13 | C++, MAC

March 2023

- Implemented the CF13 homomorphic MAC described in the paper titled, *Practical Homomorphic MACs for Arithmetic Circuits* by Dario Catalano and Dario Fiore (Eurocrypt, 2013).

### Faster Matrix Multiplication | CUDA, C++, GPU architecture

October 2022

- Optimization of large Matrix multiplication using CUDA on a Turing GPU
- The project utilized multi-threading along with instruction level parallelism to induce higher computational intensity.

### Python to WebAssembly Compiler | WebAssembly, Typescript, Python, Compiler Optimizations

May 2022

- Created a compiler as a group class project for compiling Python programs to WebAssembly which can be executed using Javascript on the browser.
- Worked on compiler optimizations such as constant folding and propagation, copy propagation, dead code elimination, hoisting using Worklist infrastructure, structured control flow using stackifier algorithm.

### $\gamma^2$ -SVP to $\gamma$ -HSVP reduction | Python, Lattices, Fplll

December 2021

- Gave and implemented the  $\gamma^2$ -Shortest vector problem (SVP) to  $\gamma$ -Hermite shortest vector problem in lattices. The idea of reduction is described in the paper *An algorithmic theory of numbers, graphs and convexity.* by Laszlo Lovasz.
- This project fills the gap in reduction and gives an implementation of the reduction.

## Teaching Assistant

---

- CSE207a: Modern Cryptography UCSD | Winter 25
- CSE107: Introduction to Modern Cryptography UCSD | Spring 22, 23, Fall 22, Winter 23, Spring 24
- CSE101: Design and Analysis of Algorithms UCSD | Summer 22
- CSE105: Theory of Computation UCSD | Fall 21