Shreyas Shivapuji

+1 (347) 452-5444 s.shreyas@nyu.edu sudorndm sudorndm.me shreyas-shivapuji

Education

New York University Sep. 2025 – May 2027 (expected)
M.S, Computer Science GPA: 3.7/4.0
Concentration: Systems and Security

Indian Institute of Technology Hyderabad Aug. 2024 – May 2025
Exchange Student GPA: 3.8/4.0
Thesis: Multi-node and Multi-GPU Scaling of FFTs

National Institute of Technology Warangal Dec. 2021 – May 2024
B.Tech, Materials Science and Engineering GPA: 3.6/4.0
Minor: Computer Science and Engineering

Research

New York University Aug. 2026 – Present
Research Student · Advisor: **Prof. Benedikt Bünz**

- Project: Efficient Validity Proofs for Bitcoin using Binary-Field SNARKs.
- Designed SNARKs for Bitcoin chain validity, enabling faster bootstrapping without relaxing trust assumptions.
- Implemented Bitcoin's consensus rules with gadgets for SHA-256, header parsing and target comparison.
- Achieved a 470 KB recursive proof attesting to all block headers since the genesis block.

New York University Feb. 2026 – Present
Research Student · Advisor: **Prof. Joseph Bonneau**

- Project: Succinct Proofs for Connection Coalescing.
- Developed a proof system to prove certificate validity for coalescable domains
- Achieved an overall bandwidth reduction of around 25×, saving additional TLS costs.
- Benchmarked and analyzed the real-world deployability of the implementation.

Indian Institute of Technology Kanpur May 2024 – Sep. 2024
Research Associate · Advisor: **Prof. Adithya Vadapalli**

- Project: Deniability and Security of Messaging Protocols.
- Designed a serverless Triple Diffie-Hellman handshake over direct IP connections, achieving an average key latency of 4 s.
- Developed a lightweight messaging client using the designed protocol.

Projects

Jolvent: Privacy-Preserving Proofs of Solvency in Jolt zkVM Feb. 2026 – May 2026

- Built a privacy-preserving solvency protocol based on Provisions using the Jolt zkVM.
- Implemented the proof-of-assets, proof-of-liabilities and solvency programs, letting an exchange prove solvency without revealing balances or addresses.

Kudzu: Simple and High-Throughput BFT Consensus Oct. 2025 – Dec. 2025

- Implemented a proof-of-concept implementation of the Kudzu BFT protocol in Rust.
- Benchmarked the protocol performance via a distributed simulation framework, achieving a minimized load-balancing CoV of 0.234.

qChat: Secure IM client using Quantum Key Distribution Aug. 2024 – Dec. 2024

- Developed a secure quantum key distribution (QKD) chat application with Python and Qiskit based on BB84 protocol.
- Implemented a hybrid end-to-end encryption framework by integrating Qiskit-simulated quantum key exchange with classical cryptography.

Teaching

New York University
Course Assistant, Basic Algorithms — Fall 2026
Grader, Theory of Computation — Spring 2026

Indian Institute of Technology Hyderabad
Course Assistant, Intro to Parallel Scientific Computing — Spring 2025

Awards and Fellowships

Best Student Thesis - UG
Dept. of MSME, IIT Hyderabad, 2025

Institute Merit Scholarship
NIT Warangal, 2021-2024

Relevant Coursework

* audited course

Graduate Honors Algorithms, Cryptography, Complexity, Information Theory, Blockchains & Cryptocurrencies, Quantum Cryptography, Encrypted Computation*

Undergraduate Parallel Computing, Quantum Computation, Data Structures and Algorithms, Database Systems, Computer Networks, Cryptography, Linear Algebra, Probability, Operations Research

Extracurricular Activities

FinWiz, NIT Warangal — Aug. 2022 – May 2024
Joint Secretary

- Team Lead of the 8-member Research Team focused on discovering market insights and novel trading strategies.
- Led the organization of the WorldQuant Brain Alphathon, a quantitative trading hackathon, in the college.

CybSec, NIT Warangal — Aug. 2022 – May 2024
Team Member

- Participated in various team CTFs and contributed to designing cybersecurity challenges for inter-college CTFs during technical fests.
- Contributed to projects such as a hacking toolkit and a customized Linux distribution for penetration testing.

Skills

Programming C, C++, Python, Rust, Go
HPC Frameworks CUDA, MPI, OpenMP, OpenACC