# UTSAV SHARMA

Mathematics and Computing
Indian Institute of Technology, Roorkee

sharmautsav0531@gmail.com
github.com/x-senpai-x
0xsenpai.substack.com

## Education

**Indian Institute of Technology, Roorkee** *2023–Present*
*BS–MS Mathematics and Computing | CGPA: 8.2/10*

**Delhi Public School, Agra (CBSE Board)** *2023*
*Senior Secondary — 94%*

## Experience

**•Ethereum Protocol Fellowship** *Consensus Layer Snarkification & Performance Analysis*
*Protocol Fellow* July 2025 - November 2025

- Benchmarked 5 zkVM architectures (RiscZero, SP1, Jolt, Zisk, Pico) for Ethereum beacon chain state transitions, identifying zisk fastest in proving and execution time
- Created **Ream-ZKVM-Benchmarks**, a Rust framework for standardized zkVM performance evaluation for Ream
- Architected **zkVM integration** for Ream's Lean Chain enabling real-time state transition verification with 6 mins proving latency

**•Enclave** *Cross-Chain Infrastructure & Intent-Based Systems*
*DeFi Backend Engineer* July 2025 - October 2025

- Architected **Magicspend++**, a cross-chain borrow-and-settle protocol
- Engineered resource locking mechanism with Turnkey, Privy, and Dynamic integration, securing transactions with zero double-spend incidents
- Built cross-chain settlement system via Circle Gateway supporting USDC transfers across 10+ chains including Ethereum, Arbitrum, Base, and Solana
- Shipped DEX aggregation layer integrating Uniswap V3 and Raydium, achieving 15% better quote optimization through multi-path routing

## Projects

**•Deimos – Mobile ZK Benchmarking Suite** *September 2025 - November 2025*
*Blockchain Society IITR* GitHub

- Created open-source mobile ZK benchmarking suite testing multiple proof systems (Circom, Noir, zkVMs) with over 6 cryptographic primitives across iOS and Android
- Measured proving time difference between mobile and desktop for equivalent circuits; findings published in benchmark reports

**•Selene Light Client** *September 2024 - December 2024*
*Blockchain Society IITR* GitHub

- Co-developed Selene, a portable Ethereum light client in Golang, implementing sync committee verification and LMD-GHOST fork choice
- Analyzed Gasper consensus protocol, documenting Casper FFG finality mechanism and cryptographic commitment schemes

**•Athena Blockchain Decoder** *September 2024 - October 2024*
*Blockchain Society IITR* EthGlobal

- Built execution trace decoder for Ethereum and Starknet in Golang, processing transactions with concurrent JSON-RPC handling
- Implemented ABI parsing supporting for automated function call interpretation

**•Zero Knowledge Proof Systems** *January 2025 - June 2025*
GitHub

- Implemented cryptographic algorithms from scratch in Rust to understand zero-knowledge proof systems
- Built core primitives: finite field arithmetic, polynomial operations, FFT, multilinear extensions, and Shamir's Secret Sharing with Lagrange interpolation, FRI protocol, sum-check, and polynomial commitment schemes.

## Technical Skills

- **Languages**: Rust, Golang, Python, Solidity,TypeScript,Circom, Noir
- **Blockchain & Cryptography**: Ethereum consensus (Gasper, LMD-GHOST), zkVMs, Zero-knowledge proofs (SNARKs, STARKs), Threshold cryptography, Cryptographic Systems
- **Protocols & Systems**: EVM, Solana VM, DeFi protocols (Uniswap, Raydium), Cross-chain protocols, Account Abstraction/Delegation (ERC-4337,7702), Intent-based protocols
- **Tools & Frameworks**: Git, Foundry, Gevm, Revm, Performance benchmarking

## Publications & Technical Writing

**Hash-Based Signature Schemes: From Lamport to FORS** *April 2025*
Technical analysis of post-quantum signature schemes

**EPF Cohort Six Writeup** *November 2025*
Deep-dive on zkVMs and Lean Ethereum

## Achievements

•**EthOnline 2024 – Nethermind Track Prize**, *September 2024*
Built Athena blockchain decoder

•**Based India Buildathon 2024 – Finalist**, *October 2024*
Built a multichain portfolio manager with a Selene as its blockchain data fetcher

•**Agentic Ethereum – Arbitrum Track Prize**, *January 2025*
Colosseum, a platform where users bet on AI Agent battles