Utkarsh Sharma

Email: utkarsh382004@gmail.com
github.com/0xnullifier
x.com/0xnullifier
0xnullifier.xyz

Education

- **Indian Institute of Technology Roorkee** Roorkee, India
  B.Tech - Electronics and Communication Engineering; CGPA: 8.045 *October 2022 - present*

  Courses: *Data structure and Algorithms, Computer Architecture, Digital Logic Design, Digital Image processing, Discrete Mathematics, Probability and Statistics, Mathematical Methods*

Experience

- **NetZero** Remote
  Grant - Mina Protocol *Jan 2025 - March 2025*
  - **Proof of Solvency on MINA**: Implemented a proof of solvency protocol on MINA. Greatly improved the UX, allowing users to easily verify their inclusion proofs in the liabilities commitment
  - **Privacy Preserving Merkle Sum Tree**: Implemented DAPOL+ Protocol with o1js primitives
  - **Proof of Asset**: A proof of asset protocol similar to provisions made non-collusive with the PLUME nullifier scheme

Open Source Work

- **Noname** Remote
  zksecurity *Jan 2025 - present*
  - **About**: Noname is a zkDSL that can have various back-end implementations like R1CS, kimchi,hi, etc.
  - **Merged PR's**: Implemented tuple type ,solved bugs in the mast, parser level. A better logging in the language with formatted strings.
  - **Open PR's**: A Sparse Merkle Tree implemented in the noname stdlib similar to circomlib.
- **Miden-Vm** Remote
  0xmiden *Jan 2025 - present*
  - **About**: miden-vm is a zkvm for the miden edge blockchain
  - **Merged PR's**: Refactoring the procedure name validation code to make it more readable, Updating lalrpop a LR1 parser in rust to the latest

Projects

- **ZeroLeaks**: Is a first of it's kind privacy preserving whistleblowing platform, Using Zk-email and a custom circuit to prove contiguous elements in an array in circom. This was built on SUI blockchain for the SUI overflow hack!
- **Zk-Fpga**: Is an implementation of Pippengers algorithm for MSM of BN254 curve in Vitis HLS as well as an NTT in goldilocks field, The core adder has a static latency of 21 cycles and can compute $2^24pointMSMin7s$
- **PriviTrade**: PriviTrade is a private perpetual trading market built on Calimero and Icp. By leveraging Calimero for secure off-chain order book management and ICP for on-chain proof verification
- **VielNetFl**: is a Federated learning platform built on NEAR blockchain for performance in rust. It implemented fault tolerance through zero knowledge krum function and has economic models for worker incentivization
- **StealTradeDAO**: is a CLOB-based Perpetual platform on MINA network made transparent through the proof of solvencies and account proofs. A chain-abstracted DAO through NEAR's chain signatures allowing people on btc to vote on a dao on ethereum
- **KeyShard**: An implementation of a distributed key generation protocol FROST based on Schnorr signatures on the fluence network
- **Hermit**: Secure MultiParty Computation Collaboration Platform built on top of Filecoin to enhance AI privacy

Achievements

- **Hackathons**
  Apr 2024 - Jan 2025
  - **Calimero x ICP**: PriviTrade won 2nd place price of $8000
  - **Akashathon**: Made AkashPay won first price in deployment track of $15000
  - **HackFS 2024**: The project KeyShard won first place in the flunece compute track bounty of $3000
  - **Movementlabs Hackathon**: MOVEx won the first place in defi track in the movement labs hackathon for a bounty worth $7000
  - **EthSingapore 2024**: Stealth Trade DAO won first place in both MINA and NEAR networks track for total bounties worth $9000
  - **Funding the commons**: VielNetFl won the first prize in NEAR track ($10000) and third in filecoin($500) at FTC 2024
  - **Archway Huntathon**: Mosaic Protocol won the second place prize of $7000
  - **Filecoin DataEconomy Hack**: Hermit is the runner up($500) in the filecoin track at FDE 2024
- **Academics**
  - Present
  - **Joint Entrance Exam**: Achieved AIR 4231 in JEE Mains and AIR 3668 in JEE Advanced 2024
  - **Department change**: Achieved a Grade Point of 9.8 (Ranked 17th in the batch of 1400 people) in the first semester, allowing for department upgrade from Mechanical Engg. to Electronics Engg.