Sivaram Dhakshinamoorthy

siv2ram@gmail.com | LinkedIn | GitHub | Substack

Education

Indian Institute of Technology, Kharagpur 2018 - 2023

B.Sc (Honours) and M.Sc (Integrated Programme) in Mathematics and Computing ***GPA**: 8.82/10*

Relevant Coursework: Foundations of Cryptography, Abstract Algebra, Probability and Statistics, and Information Theory

Research Interests: Threshold Signatures, Provable Security, and Post-Quantum Cryptography

Experience

FOSS Grant Recipient, Spiral (Block, Inc) - Remote May 2024 - Present

***FROST Signing BIP** - bitcoin/bips#2070 - siv2r/bip-frost-signing*

- Authored BIP-445 specifying the FROST signing protocol for BIP340-compatible threshold Schnorr signatures, supporting BIP32 key derivation and BIP341 Taproot tweaking.
- Built a Python reference implementation with test vector suites covering all protocol algorithms (NonceGen, NonceAgg, Sign, DeterministicSign, PartialSigVerify, PartialSigAgg).
- Opened the bitcoin/bips#2070 pull request to standardize the FROST signing protocol across Bitcoin applications.

***ChillDKG BIP** - BlockstreamResearch/bip-frost-dkg*

- Co-authored the ChillDKG BIP with Blockstream Research, specifying a secure distributed key generation protocol for FROST threshold signatures without a trusted dealer.
- Contributed to the Python reference implementation: implemented message (de)serialization, improved error handling, and created comprehensive test vectors.

***Schnorr Adaptor Signatures** - secp256k1-zkp#299 - rust-secp256k1-zkp#89*

- Rebased and extended the Schnorr adaptor signatures module in secp256k1-zkp, resolving all pending review comments and adding a Multi-Hop Locks protocol example.
- Authored Rust language bindings in rust-secp256k1-zkp, introducing type-safe Adaptor and SecretAdaptor wrapper types for the adaptor signature API.

Summer of Bitcoin Intern - Remote May 2022 - Aug 2022

Mentor: Jonas Nick, Blockstream Research - secp256k1#1134

- Selected among the top 83 out of 20,000+ applicants for the Summer of Bitcoin internship.
- Authored a Schnorr batch verification module for libsecp256k1, enabling simultaneous verification of BIP340 signatures and tweaked key checks with up to 50% speedup over individual verification.
- Reviewed secp256k1#1789, an ecmult refactor unlocking Pippenger-based acceleration; evaluated the ABCD cost model calibration through statistical analysis across 13 algorithms.

Talks

Bitshala Developer Summit - Bangalore

- Introduction to Schnorr Signatures - *slides* Nov 2024
- FROST Signing Workshop - *materials* Nov 2025

Workshops & Conferences

CryptoCamp - Lagos, Portugal by Chaincode Labs Aug 2025

- Invitation-only program for veteran bitcoiners on security proofs in public key cryptography.

Real World Crypto - Taipei, Taiwan by the International Association for Cryptologic Research (IACR) March 2026

- Attended the main event and affiliated workshops on MPC (RWMPC), open-source cryptography (OSCW), and post-quantum (RWPQC).

Mentorship

Summer of Bitcoin, libsecp256k1 May 2023 - Aug 2023

- Co-mentored a student through an open-source contribution to the libsecp256k1 cryptography library.

GirlScript Summer of Code May 2021 - Aug 2021

- Introduced 15–20 students to their first open-source contributions through structured onboarding guides, labeled beginner issues, and active code review.