Bharath Namboothiry

brn@stanford.edu | (503) 989-2001 | namboothiry.com

EDUCATION

University of Pennsylvania — **Philadelphia, PA**
Ph.D. in Computer and Information Science — *Class of 2029*
Specializing in Applied Cryptography | Advised by Prof. Pratyush Mishra
- **Awards:** Named Doctoral Fellow (2024)

Stanford University — **Stanford, CA**
M.S. in Computer Science with Specialization in Theory | GPA: 4.00 — *Class of 2024*
B.S. in Mathematics with Minor in South Asian Studies | GPA: 3.97
- **Programming Languages:** Rust, Python, C/C++, JavaScript, LaTeX
- **Extracurricular Leadership:** Residential Advisor (RA), Calculus Tutor, Stanford Bhangra Team, Blyth Fund Pitch Lead

RECENT PROJECTS

db-SNARK: Efficiently Verifiable SQL — *Aug 2024 – Present*
- Developing a cryptographic proof system for SQL verification using Polynomial Interactive Oracle Proofs, ensuring tamper-proof and verifiable queries.
- Optimizing the query planner for proof generation, reducing prover overhead while maintaining efficient query execution in critical database systems.
- Improving proof efficiency of relational algebra operations to expand the space of verifiable queries

LockBox: Time-Locked Commitments for Sealed Bid Auctions — *Aug 2024 – Present*
- Designing a new time-lock commitment scheme puzzle, that enables message recovery without the committer's involvement
- Ensuring accountability in distributed sealed bid auctions by providing the auctioneer a way to recover disconnected bids
- Enhancing fairness in the auction process by eliminating the possibility of discarding unfavorable bids

Cryptographic Memory Tagging: Towards Stateless Integrity — *Jan 2024 – Aug 2024*
- Developed a stateless memory safety mechanism that embeds cryptographic tags within memory pointers, reducing reliance on metadata storage and lowering performance overhead
- Implemented entropy-based verification, achieving access control coverage with minimal overhead over SPEC CPU tests, demonstrating scalability and efficiency

Revealable Functional Commitments — *June 2022 – June 2023*
- Developed new primitives to functional commitment schemes, enabling partial reveals of private committed functions
- Expanded the state-of-art, allowing function privacy to be dynamically adjusted with zero-knowledge guarantees

PROFESSIONAL EXPERIENCE

Intel Labs — **Santa Clara, CA**
Graduate Research Intern - Cryptography — *Jan 2024 – Aug 2024*
- Collaborated on DARPA's HARDEN initiative to enhance the security of integrated computing systems via lightweight crypto
- Furthered Cryptographic Capability Computing (C3), which optimizes vulnerable metadata with partially encrypted pointers

Stanford Theory Group — **Stanford, CA**
Researcher, Applied Cryptography Group — *June 2021 – Dec 2023*
- Researched under the advisements of Profs. Dan Boneh, Li-Yang Tan, and Moses Charikar
- Led collaborative and solo research projects in ZK proof systems, multiparty compute, graph theory and complexity theory

Stanford School of Engineering — **Stanford, CA**
Course Assistant — *Sept 2022 – Dec 2023*
- Mentored and instructed a total of 1000+ students in cryptography and algorithms courses using C++, JS, and Solidity
- Managed teams of 15+ staff to prepare, evaluate, and revise course material, homework, and exams
- Developed and shared solutions to close the gap between student needs and instruction in theoretical computer science

Intel Corporation — **Hillsboro, OR**
Platforms and Systems Intern — *June 2020 – Sept 2020*
- Led the thermal characterization of mobile PC platforms as an effort bottleneck problem, in collaboration with senior engineers
- Automated a DOE system for thermal engineers using Python and FloScript, reducing experiment times from days to minutes

Lighthaven Capital Management — **San Francisco, CA**
SWE & Equity Research Intern — *Jan 2020 – Sept 2020*
- Directed a team of university interns involved in fundamental stock research, in-depth equity evaluation and technical analysis
- Built Python-based web tools that accelerated stock screening and instantly visualized Lighthaven's unique research pipeline