Benjamin Sepanski

Houston, TX | ben.sepanski@gmail.com | https://bensepanski.github.io

Skills

Programming Languages

Rust, Python, Solidity, EVM, C++/CUDA, TypeScript, Java, Go
(some experience with) x86_64 Assembly, R

Libraries & DSLs

circom, halo2, o1js, gnark, risc0, corset (Linea)
(some experience with) arkworks, NEAR, AWS Nitro, Dynamo DB

Software & Tools

Git, Unix shell, LaTeX, GitHub Actions CI/CD, Semgrep, poetry/pip, foundry, hardhat
(some experience with) afl++, HSMs, Maven, CMake, Nix, Docker

Education

University of Texas at Austin — *August 2020 – December 2022*

M.S. in Computer Science, *GPA*: 4.0
Studied and researched programming languages in the UToPiA group
Advisor: Dr. Isil Dillig

Baylor University — *August 2016 – May 2020*

B.S. in Mathematics, Minor in Computer Science, *GPA*: 4.0
45 hours of graduate coursework in mathematics, computer science, and statistics
Advisor: Dr. Robert Kirby

Work Experience

Chief Security Officer — *March 2024 – Present*
VP of Auditing — *July 2023 – March 2024*
Research Scientist — *January 2023 – July 2023*

Veridise

- Performed over 35 manual source code security reviews for clients, finding dozens of high/critical bugs in a variety of emerging technologies.
- Reviewed cryptographic implementations of distributed signing schemes (FROST), elliptic curve operations, ECDSA, Keccak, sponge-based encryption, and recursive ZK-verifiers.
- Reviewed ERC 4626 Vaults, NFT collections, over-collateralized lending protocols, AMMs, orderbooks, token implementations, zkEVMs, and execution layers across a variety of ecosystems including EVM chains, Mina, Linea, Monero, and NEAR.
- Hired and managed an auditing department, growing a team of one to a team of seven.

- Created project timelines and quotes for over 400 potential projects, tracking the setup and delivery of over 75 projects, and developing an internal quoting Python library.
- Set revenue goals, determined pricing strategy, and managed the hiring budget for the auditing department. Managed internal revenue allocation for the company.
- Interacted with potential clients to explain services and collect project requirements.
- Regularly met with the executive team to determine company strategy, prepare go-to-market plans for security software releases, and select target technologies.

Research Scientist *May 2021 – August 2021*

Lawrence Berkeley National Laboratory

- Extended C++/CUDA high-performance data layout Bricks library to reduce metadata usage, support complex types, and compute FFTs using NVIDIA's cuFFT library.

Undergraduate Research Assistant *January 2019 – August 2020*

Baylor University

- Applied nonlocal boundary integral equations to support finite element methods on wave equations in an unbounded domain.
- Developed, tested, and integrated research into Python library meshmode.

Director's Summer Program Participant *May 2018 – August 2018*

Director's Program at the National Security Agency

- Received Top Secret // Sensitive Compartmented Information clearance.
- Applied language modeling and n-gram techniques to a high-priority classified project.

Publications

Synthesizing fine-grained synchronization protocols for implicit monitors (with Dr. Kostas Ferles, Rahul Krishnan, Dr. James Bornholt, and Dr. Isil Dillig) Proc. ACM Program Lang. 6, OOPSLA1, 2022

"Maximizing Performance Through Memory Hierarchy-Driven Data Layout Transformations," (with Dr. T. Zhao, Dr. H. Johansen and Dr. S. Williams) in *2022 IEEE/ACM Workshop on Memory Centric High Performance Computing (MCHPC), Dallas, TX, USA, 2022*

Finite Elements for Helmholtz equations with a nonlocal boundary condition (with Dr. Robert Kirby and Dr. Andreas Klockner) SIAM Journal on Scientific Computing, 2021

Augmented Hilbert series of numerical semigroups (with Christopher O'Neill, Jeske Glenn, and Vadim Ponomarenko) Integers 19 (June 3, 2019), #A32

Selected Awards and Honors

2020 Department of Energy Computational Science Graduate Fellow
2019 Goldwater Scholar