

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, LLVM, DynamoDB

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.
- Set up and ran internal and third-party static analyzers and fuzzers for multiple clients during code reviews.
- 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.
- Developed detectors for a static analyzer built on LLVM.
- 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, tracked the setup and delivery of over 75 projects, and developed Python libraries for quoting and audit report generation.
- 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

- DOE CSGF Practicum supervised by Dr. Samuel Williams and Dr. Hans Johansen.
- Extended C++/CUDA high-performance data layout Bricks library to reduce metadata usage, support complex types, and compute FFTs using NVIDIA's cuFFT library.
- Used roofline analysis and the Bricks layout to optimize high-dimensional stencil computations from the GENE code—a phase-space SciDAC Fusion Code.

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 with Dr. Robert Kirby and Dr. Andreas Klockner.
- 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 with Agency special background investigation and full scope polygraph examination.
- Submitted detailed findings in an internal refereed technical paper.
- Designed, implemented, and tested graph optimization algorithms.
- Applied and extended language modeling and n-gram techniques to a high-priority classified project.

Research Assistant

May 2017 – August 2017

Research Experience for Undergraduates at San Diego State University

- Researched Numerical Semigroups at San Diego State University.

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

Recipient of Mathematical Association of America (MAA)'s Student Travel Grant to the 2018 Joint Mathematics Meetings

2018 & 2019 Outstanding Math Student at the J. Harry and Anna Jeanes Academic Convocation

Recipient of Baylor Mathematics Scholarships

Jerry Johnson Scholarship (2018 & 2019)

KL & Vivian Carter Scholarship (2017)

Schultz-Werba Math Scholarship (2017)

Gene & Ruth B Royer Scholarship (2018 & 2019)

Howard / Anita Rolf Scholarship (2017)

Carlile Engineering Scholarship (2016)

Received President's Gold Scholarship at Baylor University

National Merit Scholar (2016)