# A. References

Jamie Finnigan | Director of Product Security, HashiCorp
jfinnigan@hashicorp.com

Erinmichelle Perry | Chief Information Security Officer, Spotify
erinmichellep@spotify.com

Shems Abdelwahab | Senior Program Manager, Open Technology Fund
shems@opentech.fund

Tim Lisko | Senior Director, IT & Security Engineering, DigitalOcean
tlisko@digitalocean.com

Nicolas Patry | Machine Learning Engineer, Hugging Face
nicolas@huggingface.co

John Mardlin | Security Engineer, OP Labs
john@oplabs.co

Jay Prakash | CEO, Silence Laboratories
jay.prakash@silencelaboratories.com

Howard Wu | CTO, Provable
howard@provable.com

# B. Key Personnel

The project team is chosen based on each engineer's skill set and availability. Personnel may vary for this project.

## Cryptography Team

### Jim Miller, Engineering Director, Cryptography

Jim is a principal security engineer and engineering director of our cryptography team, through which he applies his knowledge of cryptography to exciting, cutting-edge research projects and assurance projects with advanced cryptographic protocols. Jim spent two years in a cryptography PhD program at Yale University. At Yale, Jim researched lattice-based verifiable computation and other lattice-based cryptographic research problems. Since joining Trail of Bits, Jim has reviewed a wide spectrum of cryptographic software, including a novel encrypted hard drive developed by Western Digital, Hashicorp's Vault, and several novel applications of advanced cryptographic protocols such as multi-party computation and zero-knowledge proofs. Jim has experience in reviewing these protocols across many languages and integrating static and dynamic analysis tools such as fuzzing.

Selected Publications:

- "ECDSA: Handle with Care" (blog post)
- Western Digital's Sweet B Security Assessment (security review)
- Weak Fiat-Shamir Attacks on Modern Proof Systems (publication)

GitHub: https://github.com/james-miller-93

### Fredrik Dahlgren, Principal Security Engineer

Fredrik Dahlgren is a principal security engineer on the Trail of Bits Cryptography Team. He has multiple years of experience reviewing novel cryptographic protocols and implementations of everything from threshold signature schemes and zero-knowledge proof systems to end-to-end encrypted messaging applications and encrypted hard drives. Fredrik is also the main developer behind Circomspect, a static analyzer and linter for the Circom zero-knowledge domain-specific language. Before joining Trail of Bits, Fredrik worked for twelve years as a Security Researcher and Cryptographer for the Swedish government. He holds a Ph.D. in Mathematical Logic and a Master's degree in Mathematics and Computer Science from Uppsala University.

### Tjaden Hess, Senior Security Engineer, Cryptography

Tjaden Hess is a security engineer on the Trail of Bits cryptography team. He performs security reviews of cryptography-heavy applications including threshold signing, multiparty computation, zero-knowledge proof systems and circuits, and HSM applications. Beyond auditing, he produces documentation and tools that make it easy for engineers to write secure cryptographic applications. Tjaden is currently working on production-ready SMT-solving tools for arithmetic circuits and specification for zero knowledge proofs at https://www.zkdocs.com/

Prior to joining Trail of Bits in May 2022, Tjaden's work experience includes:

- Apple: RTL-level formal verification, designing SystemVerilog models and proof procedures for clock gating and GPU memory architectures.
- Green Hills Software: C/C++ compiler test engineering; fuzzing, optimization and new feature validation and signoff. RTOS validation, testing and security review.
- BA in Math + CS, Cornell University (2020)
- Tjaden is an author of ERC-4337 and EIP-152.

### Filipe Casal, Principal Security Engineer, Cryptography

Filipe Casal is a principal security engineer at Trail of Bits. He mainly focuses on security reviews of cryptography projects such as threshold signature schemes and zero-knowledge proof systems. While preparing for these assessments, he builds tools to help audit code. He has created ZKDocs, an interactive documentation on zero-knowledge proof systems and related primitives, Amarna, a static-analyzer and linter for the Cairo programming language, and weAudit, a collaborative code review tool for VSCode.

Before joining Trail of Bits, he was an invited assistant Professor at the University of Lisbon, teaching and researching on type theory, satisfiability procedures, and probabilistic logics with applications to security.