# Bhargava Shastry

Security Engineer & Researcher — Ethereum protocol security, differential fuzzing

bshastry@posteo.de
bshastry.github.io · github.com/bshastry
keybase.io/bshastry (PGP) · Remote

## EXPERIENCE

**Security Engineer** · Ethereum Foundation 2019 – present

- Coverage-guided differential fuzzing of state-test execution across geth, Besu, Nethermind, Erigon, and revm; upstream fixes merged in Erigon, Nethermind, revm, and ethereum/execution-specs.
- Hard-fork readiness testing (gas repricing, block-level access lists, new EIP semantics) validated against the executable specs.
- Technical evaluator for the Ethereum Foundation bug bounty program: reproduction, severity assessment, and cross-client blast-radius analysis of execution- and consensus-layer reports.
- Differential testing of post-quantum standards: cross-checking ML-KEM (FIPS 203) and ML-DSA (FIPS 204) implementations (mlkem-native, BoringSSL, libcrux, CIRCL).
- Earlier: core contributor to Solidity compiler testing — 300+ commits, ABI encoder v2 differential fuzzer, 25 miscompilation bugs documented in the SolSmith paper (arXiv:2607.07217).

**Independent Security Researcher** · Freelance 2017 – present

- Contributions to Google's OSS-Fuzz (69 commits) and Open vSwitch security testing; built orthrus, a framework for managing parallel fuzzing campaigns.
- Security testing of Ethereum P2P stacks: rust-libp2p fuzzing, yamux/mplex multiplexer stress testing, wire-protocol (eth/6x, snap/1) fixes.

**Security Researcher** · Fraunhofer Secure IT 2011 – 2012

Android platform security: privilege-escalation defenses and lightweight domain isolation. Published at NDSS and ACM SPSM.

**Software Engineer** · Ittiam Systems 2007 – 2008

Software and tests for Ittiam's Voice-over-IP phone software.

## EDUCATION

**Ph.D. in Computer Science** · Technische Universität Berlin 2013 – 2019

Static analysis and fuzzing techniques for open-source bug detection.

**M.Sc. in Computer Science** · EPFL, Lausanne 2008 – 2010

Security of microcontrollers and embedded systems.

**B.Tech. in Electrical Engineering** · National Institute of Technology Karnataka 2003 – 2007

## SELECTED PUBLICATIONS (11 total — full list at bshastry.github.io)

Finding and Understanding Miscompilation Bugs in the Solidity Compiler. arXiv:2607.07217, 2026.

Taking Control of SDN-based Cloud Systems via the Data Plane. Symposium on SDN Research 2018. **Best Paper Award**

Static Program Analysis as a Fuzzing Aid. RAID 2017.

Static Exploration of Taint-Style Vulnerabilities Found by Fuzzing. USENIX WOOT 2017.

Towards Vulnerability Discovery Using Staged Program Analysis. DIMVA 2016.

Towards Taming Privilege-Escalation Attacks on Android. NDSS 2012.

## TALKS

Trust No Single Witness: Differential Fuzzing & Bug-Bounty Triage for Ethereum Clients. Berlin Ethereum Day, 2026.

Fuzzing the Solidity Compiler. Devcon 5 (Osaka, 2019); EthCC 3 (Paris, 2020); FuzzCon EU (2020).

## SKILLS

| | |
|---|---|
| **Security** | Differential fuzzing, protocol security, bug bounty triage, post-quantum cryptography, static analysis |
| **Languages** | Go, Rust, C/C++, Python, Solidity |
| **Tooling** | goevmlab, libFuzzer, cargo-fuzz, AFL, Slither, Foundry, OSS-Fuzz, Docker, LLM agent orchestration |

Public artifacts — merged fixes, upstreamed tests, and publications — are linked at bshastry.github.io#findings. Last updated July 2026.