Ilia Vlasov

aili.dev | elijah.vlasov@gmail.com | LinkedIn | GitHub

Professional summary

Experienced software engineer and researcher with solid math and logic background. Avid problem-solver targeting the hardest problems varying across different areas. Fluent in various programming languages, particularly those with strong memory-security guarantees — Rust and Haskell. Cryptography and privacy-enhancing technologies enthusiast. Experienced in formal verification of cryptographic applications. Capable of working in a dynamically changing environment and constantly learning about cutting-edge technologies. Dedicated to delivering high-quality innovative results. Passionate about working on low-level intricacies of software systems. Highly strategic, team player, fresh project owner. Open-source contributor.

Technical Skills

Programming languages: Rust, Haskell, Golang, C/C++, Python, Java.
Database management systems: SQLite, MySQL, PostgreSQL, Redis.
Backend frameworks: Django, Spring.
Cryptography: Public-key encryption, cryptographic hash functions, SNARKS/STARKS, Lattice-based cryptography.
Zero-knowledge languages and frameworks: Circom, Halo2, Plonky3.
Developer Tools: git, bash scripting, Docker, Kubernetes, Github CI/CD actions, vim.

Experience

Cryptography Researcher and Formal Verification Engineer Mar 2022 - Present
Nethermind *London, UK*

- Desinging and optimising cryptographic protocols.
- Leading a team of 5 engineers implementing cryptographic protocols.
- Formally verifying security properties of zero-knowledge protocols.

Research Engineer Aug 2021 - Feb 2022
Sofoil *Kazan, Russia*

- Participated in the development of a training simulator for petroleum geologists called PolyPlan.
- Developed from scratch a microservice that performs calculation of pressure build-up/fall-off in oil wells in the presence of external factors using Python. Assisted senior researchers in developing mathematical models of such behaviour.

Teaching assistant Jan 2021 - Jul 2021
The University of Western Ontario *London (ON), Canada*

- Assisted with Linear Algebra and Mathematical Logic courses.
- Held office hours for first-year undergraduate students.

Projects

LatticeFold | *Rust, Rayon, unsafe Rust, zkSNARKS, lattice-based cryptography.* Jun 2024 - Dec 2024

- Led the implementation of the first lattice-based cryptographic folding scheme called LatticeFold in Rust.
- Worked on researching opportunities to apply the scheme in the context of scalable transparent arguments of knowledge (STARKs).
- Worked on a derived folding scheme called OvaL (not yet public).

Mova folding scheme | *Rust, Rayon, zkSNARKS, verifiable computation.* Jun 2024 - Aug 2024

- Co-authored the paper describing the protocol.
- Led the proof-of-concept implementation in Rust.

Verified PLONK verifier | *Solidity, Yul, EasyCrypt, SMT solvers, zkSNARKS.* Jul 2024 - Sep 2024

- Participated in functional formal verification of a PLONK/plookup Yul verifier used by zkSync.

Formally verified Risc0 zkVM | *Lean4, C++, MLIR, zk circuits, RISC-V.* Jun 2023 - Aug 2023

- Proving formal correctness of zk circuits implementing a zero-knowledge RISC-V virtual machine.
- Proving correctness of the instruction decoder in the CPU execution pipeline.

Cairo virtual machine in golang | *golang, Cairo.* Sep 2023 - Oct 2023

- Implementing the first sketch of the virtual machine.
- Worked on optimising parts involving finite field arithmetic.

Clear, the Solidity verification tool | *Haskell, Lean4, Solidity, EVM bytecode, Yul.* Sep 2023 - Jan 2024

- Worked on developing a formal verification harness for Solidity smart-contract language in Haskell/Lean4.

Horus SMT-checker for Cairo language | *Haskell, Python, Cairo, SMT solvers.* Mar 2022 - Feb 2023

- Led development of the compiler plugin in Python that prepares data for the SMT-solver core component.
- Participated in development of the core SMT-solving component in Haskell.

Education

Kazan Federal University Kazan, Russia
Master of Science in Mathematics *Sep 2018 - Jul 2020*

Kazan Federal University Kazan, Russia
Bachelor of Science in Mathematics *Sep 2014 - Jul 2018*

References

Available on Request