https://yoichihirai.com
i@yoichihirai.com

Dr. Yoichi Hirai

Professional Experience

2024-2025 Member of Technical Staff at Nexus Laboratories Inc., involving a RISC-V zkVM[1].

2020-2024 Senior Software Engineer at BedRock Systems, Inc., involving Coq verification of C++ programs with concurrency.

2018-2019 Engineer at brainbot technologies AG, involving Solidity.

2016-2018 Formal Verification Engineer at Ethereum DEV UG, involving specification of Ethereum Virtual Machine in Isabelle/HOL and proofs about a distributed algorithm (like accountable safety).

2014-2016 Formal Verification Engineer at FireEye, Inc., involving formal verification in Coq and model-based testing of a microkernel.

2013-2014 Researcher at Highly Reliable Software Group in AIST.

2010–2011 Research assistant at IIJ Innovation Institute, involving a Coq proof about Haskell's Data.Map library.

2006–2009 Part-time programmer for Kokolink, Co., involving analysis and modification of PostgreSQL.

Natural Languages Japanese (native), English (fluent), German (advanced).

Publication

Refereed Papers (Selected)

[1] Yoichi Hirai: Defining the Ethereum Virtual Machine for Interactive Theorem Provers. In *Financial Cryptography Workshops 2017*, LNCS 10323, pp. 520–535. 2017.

[2] Hanno Becker, Juan Manuel Crespo, Jacek Galowicz, Ulrich Hensel, Yoichi Hirai, César Kunz, Keiko Nakata, Jorge Luis Sacchini, Hendrik Tews, Thomas Tuerk: Combining Mechanized Proofs and Model-Based Testing in the Formal Analysis of a Hypervisor In *FM 2016*, LNCS 9995, pp. 69–84. 2016.

[1] I didn't use my GitHub account but you can find "Yoichi Hirai" in the commit history.

[3] Yoichi Hirai: An Intuitionistic Epistemic Logic for Sequential Consistency on Shared Memory. In *LPAR-16*, LNAI 6355, pp. 272–289. Springer. 2010.

[4] Alessandro Facchini, Yoichi Hirai, Maarten Marx, Evgeny Sherkhonov: Containment for Conditional Tree Patterns. In *Logical Methods in Computer Science* **11**(2). 2015.

Theses

[5] Yoichi Hirai: Hyper-Lambda Calculi, Doctoral Thesis, 2013.

[6] Yoichi Hirai: An Intuitionistic Epistemic Logic for Asynchronous Communication, Master's Thesis, 2010. Work supervised by Prof. Masami Hagiya.

Programming Languages

proficient Rocq (previously called Coq) (ssreflect, Iris), C++.

professional Rust, Python

used ACL2, Scheme, OCaml, VHDL, Isabelle/HOL, SysML, Haskell, C, Solidity, Ethereum Virtual Machine, Alloy.

Open Source Contribution under Username @pirapira

eth-isabelle A formalization of Ethereum Virtual Machine, which can be translated into Coq, Isabelle/HOL and OCaml.

Proof-of-Stake formal methods
Isabelle/HOL proofs about a distributed algorithm.

Yellow Paper
Many fixes in the specification of Ethereum.

bamboo A compiler from a state-machine based language into Ethereum Virtual Machine.

ethereum/tests
The test suite for Ethereum Virtual Machine.

Education, Distinction PhD (computer science), the University of Tokyo. Classified among the 20 best candidates in Japanese Mathematical Olympiad.