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

Dr. Yoichi Hirai

Professional Experience

2024	Senior Software Engineer at Nexus Laboratories Inc., involving formal verification of arithmetic circuits for succinct arguments.
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 Ethereum application development.
2016-2018	Formal verification engineer at Ethereum DEV UG, involving specification of Ethereum Virtual Machine in Isabelle/HOL and Isabelle/HOL proofs about a distributed algorithm.
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 (a Japanese national institute), involving requirement-analysis and SysML modelling of transportation systems and Coq proofs about data encoding.
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, TestDaF level 4).

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.

[3] Yoichi Hirai and Kazuhiko Yamamoto: Balancing Weight-Balanced Trees. *Journal of Functional Programming*, **21**(03), pp. 287–307. 2011.

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

[5] Yoichi Hirai: A Lambda Calculus for Gödel–Dummett Logic Capturing Waitfreedom, In *FLOPS 2012*, LNCS 7294, pp. 151–165. 2012.

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

Theses

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

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

Programming Languages

proficient Coq (ssreflect, Iris), C++.

used Scheme, OCaml, Isabelle/HOL, SysML, Haskell, Python, 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
An Alloy analysis and Isabelle/HOL proofs about a distributed algorithm.

Yellow Paper
Many fixes in the specification of Ethereum.

raiden-contracts
: Onchain component of Raiden payment network.

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

Solidity
: A compiler from a contract-oriented language Solidity into Ethereum Virtual Machine.

ethereum/tests
: The test suite for Ethereum Virtual Machine.

Education

2010–2013 PhD course in computer science, the University of Tokyo.

2011–2012 Visiting student at ILPS, the University of Amsterdam.

2008–2010 MSc in computer science, the University of Tokyo.

2004–2008 BSc in information science, the University of Tokyo.

Awards/Distinctions/Research Funding

2011–2013 JSPS Research Fellowships for Young Scientists.

2010 Dean's Award.

2002 Classified among the 20 best candidates in Japanese Mathematical Olympiad.