HOL4 users' workshop

Tuesday 25th – Wednesday 26th June 2024

Arm, Cambridge, UK

Contact: Hrutvik Kanabar, hrutvik.kanabar2@arm.com

List of attendees

Alex Joseph Coleman	*University of Kent, UK*
Andreas Lindner	*KTH, Sweden*
Andreas Lööw	*Imperial College London, UK*
Anthony Fox	*Arm*
Anoud Alshnakat	*KTH, Sweden*
Didrik Lundberg	*KTH, Sweden*
Eleni Vafeiadi Bila	*Arm*
Henrik Akira Karlsson	*KTH, Sweden*
Hrutvik Kanabar	*Arm*
Hugo Vincent	*Arm*
Jade Alglave	*Arm*
Magnus Myreen	*Arm*
Michael Norrish	*ANU, Australia*
Milad Ketabi	*University of Surrey, UK*
Ramana Kumar	*unaffiliated*
Robert Soeldner	*University of York, UK*
Roberto Guanciale	*KTH, Sweden*
Shale Xiong	*Arm*
Thibaut Pérami	*University of Cambridge, UK*
Thomas Bauereiss	*University of Cambridge, UK*
Yong Kiam Tan	*unaffiliated*

Programme – day 1

09:00–09:30 **Arrival and admission**

09:30–10:15 **Specifications and theorem-proving @ Arm** ***opening***
Anthony Fox (Arm)

10:15–11:15 **HOL4 State of the System** ***keynote***
Michael Norrish (ANU, Australia)
I will describe the state of the system both in terms of the code base as it exists and trying also to describe existing projects working over that foundation. I will also describe more or less speculative ideas for future work. All of this discussion will be structured around the kernel, tools and libraries above the kernel, and our (core and example) theories.

11:15–11:45 **Break**

11:45–12:15 **Proof-Producing Symbolic Execution of Intermediate Language BIR for RISC-V Binary Verification**
Andreas Lindner (KTH, Sweden)
I will briefly introduce the symbolic execution inference rules we developed and proved correct. Further, I will give a brief overview of how these have been instantiated for BIR (HolBA) and used for verification of simple Cortex-M0 and RISC-V programs. All has been implemented in HOL4 and we are currently working on improving automation and scalability of the proof-producing procedures to apply this work to larger and more complex programs. I will conclude by reporting on our current benchmarks.

12:15–12:30 **HOL4P4: Semantics and Type System for Data Planes**
Anoud Alshnakat (KTH, Sweden)
In this presentation, I will discuss Software-Defined Networking (SDN) and explore its data planes that handle packet processing. Then I will introduce P4, a domain-specific language specifically designed for programming these data planes. Then I will discuss the formalization of P4 language and type system in HOL4.

12:30–12:45 **P4 Executable Semantics and Symbolic Execution**
Didrik Lundberg (KTH, Sweden)
I will describe the development of shallow-embedded symbolic execution facilities for HOL4P4, as well as the HOL4P4 import tool for P4 programs. The focus will be on handling peculiarities of P4 in the symbolic reasoning and scaling the methods to real-world, industry-size programs.

12:45–13:45 **Lunch**

Programme – day 1 (continued)

13:45–14:30 **Verification of the Realm Management Monitor ABI**
Eleni Vafeiadi Bila and Anthony Fox (Arm)

14:30–15:00 **Validation of Arm feature configurations**
Magnus Myreen (Arm)

15:00–15:30 **Break**

15:30–16:00 **Covering the Last Mile in Trustworthy Automated Reasoning with CakeML**
Yong Kiam Tan (unaffiliated)
The CakeML project has grown from its beginnings as a formally verified compiler for an ML-like language to a full ecosystem today capable of producing various end-to-end verified applications.
This talk will start with an introduction to CakeML, including its compiler's novel verified bootstrapping process. Then, I will outline how the CakeML ecosystem can be used to build verified proof checking tools that are capable of efficiently scrutinizing the outputs of automated reasoning solvers. By developing these checkers in close collaboration with tool developers, CakeML can provide practical proof checking for various automated reasoning theories with a remarkably small and shared trusted base.

16:00–16:30 **`cv_transLib`: using fast computation in HOL4**
Magnus Myreen (Arm)

16:30–16:45 **The current state of Verilog semantics modelling in HOL4**
Andreas Lööw (Imperial College London, UK)
I will give a summary of my previous work and ongoing work on Verilog-based hardware development inside HOL4. This work includes a formalisation of the Verilog standard and also proof-producing and verified tools for Verilog development and synthesis inside HOL4. I will highlight some of the problems of the Verilog standard I have run into while formalising it.

19:00 **Workshop dinner @ Giggling Squid**

Programme – day 2

09:00–09:30	**Arrival and admission**	
09:30–10:30	**Tips and tricks** Michael Norrish (ANU, Australia)	
10:30–11:00	**Break**	
11:00–12:00	**Proof clinic**	***plenary***
12:00–13:00	**Lunch**	
13:00–13:45	**Writing formal specifications at Arm** Jade Alglave (Arm) *In this talk we will give an overview of the progress made by the Arm Architecture Formal Team on writing formal specifications. Initially focussed on the memory model, we have recently expanded our work to writing a definition for ASL, the Architecture Specification Language used at Arm to describe how instructions behave. We will talk about both those areas and present our work to date.*	
13:45–14:15	**Towards HOL4 verification of ASL specifications** Hrutvik Kanabar (Arm)	
14:15–15:15	**HOL4 wish-list**	***plenary***
15:15–15:45	**Break**	

Programme – day 2 (continued)

15:45–16:15 **Verifereum: Formal Verification of Ethereum Applications**
Ramana Kumar (unaffiliated)
Work in progress and future/proposed work. Seeking collaborators.

16:15–16:30 **Type-based information declassification**
Alex Coleman (University of Kent, UK)
In this talk I will present D2CC, a new modal type theory for information declassification. We build upon the seminal work of Abadi et al., the Dependency Core Calculus (DCC) that already has a monad for classification of information. D2CC inherits the classification monad from DCC, but also adds a new modality for allowing declassification. We build a logical relation model describing both the unary and relational semantics of these modalities (including other types), and use it to prove the soundness (an indistinguishability-based hyper-property) of D2CC. We also describe the conditions under which our new modality forms a comonad, and prove the corresponding comonad laws for it. This work is being formalised in HOL.

16:30–16:45 **Lightning talks**

- ***Formal Verification of Correctness and Information Flow Security for an In-Order Pipelined Processor***

  Roberto Guanciale (KTH, Sweden)

  A short talk on the 5-stage pipeline verified in HOL.

- ***Executable Multicore Model of RISC-V in HolBA***

  Henrik Akira Karlsson (KTH, Sweden)

  Work-in-progress executable model of multicore RISC-V implemented in HolBA/HOL4. The model lets us (1) prove properties of RISC-V code executed with a bounded number of steps, and (2) validate a relational multicore RISC-V model by the execution of litmus tests. Currently working on proving the final theorems relating the executable with the relational model. The model can easily be extended to ARM.

16:45–17:00 **Closing**