NICTA

The seL4 microkernel verification

QED+20, Vienna

Gerwin Klein

Australian Government
Department of Broadband, Communications and the Digital Economy
Australian Research Council

NICTA Funding and Supporting Members and Partners
Australian National University · UNSW · NSW Trade & Investment · Victoria · The University of Melbourne · The University of Sydney · Queensland Government · Griffith University · QUT · The University Of Queensland

Isolation

Isolation is the Key

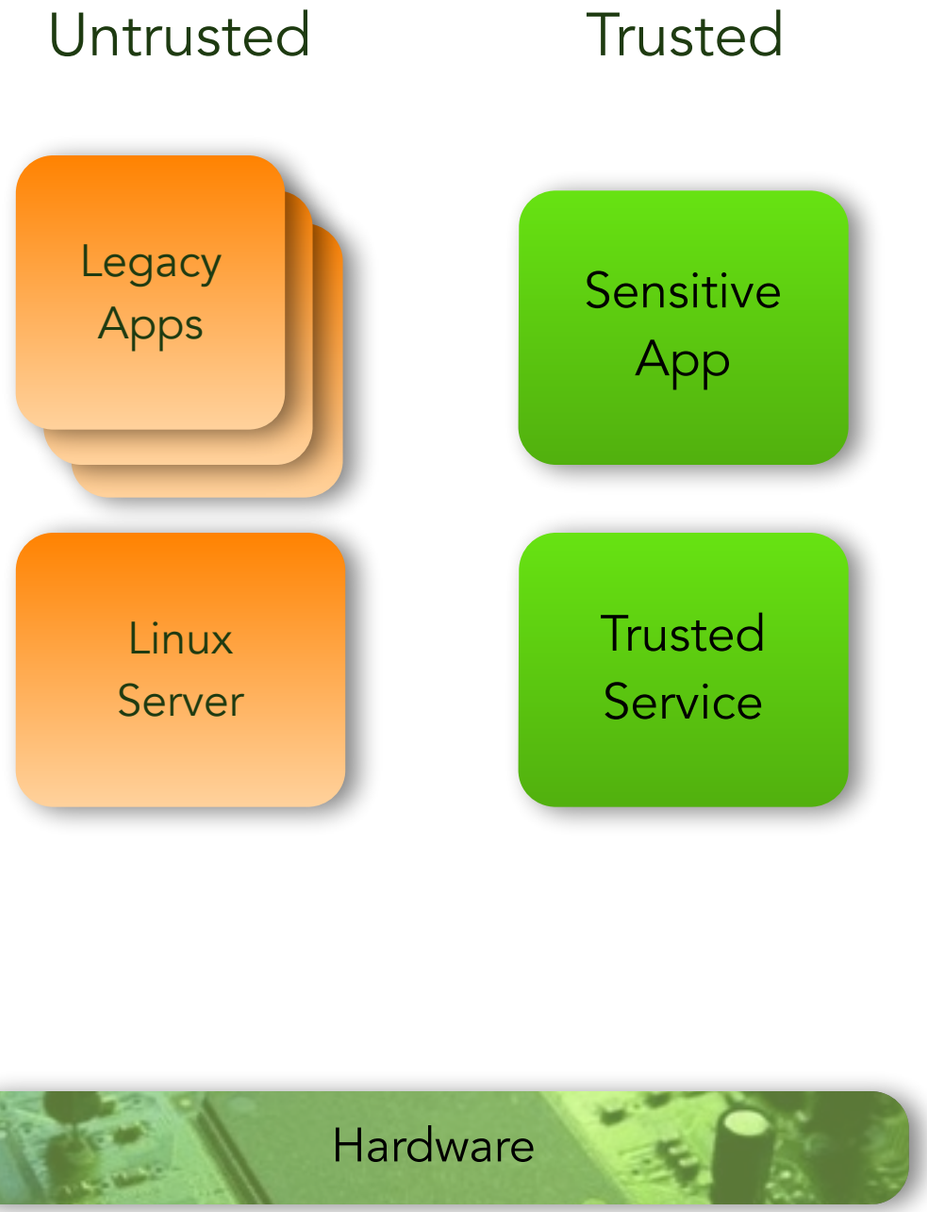
Trustworthy Computing Base

- message passing
- virtual memory
- interrupt handling
- access control

Applications

- fault isolation
- fault identification
- IP protection
- modularity

Trusted next to Untrusted



Isolation is the Key

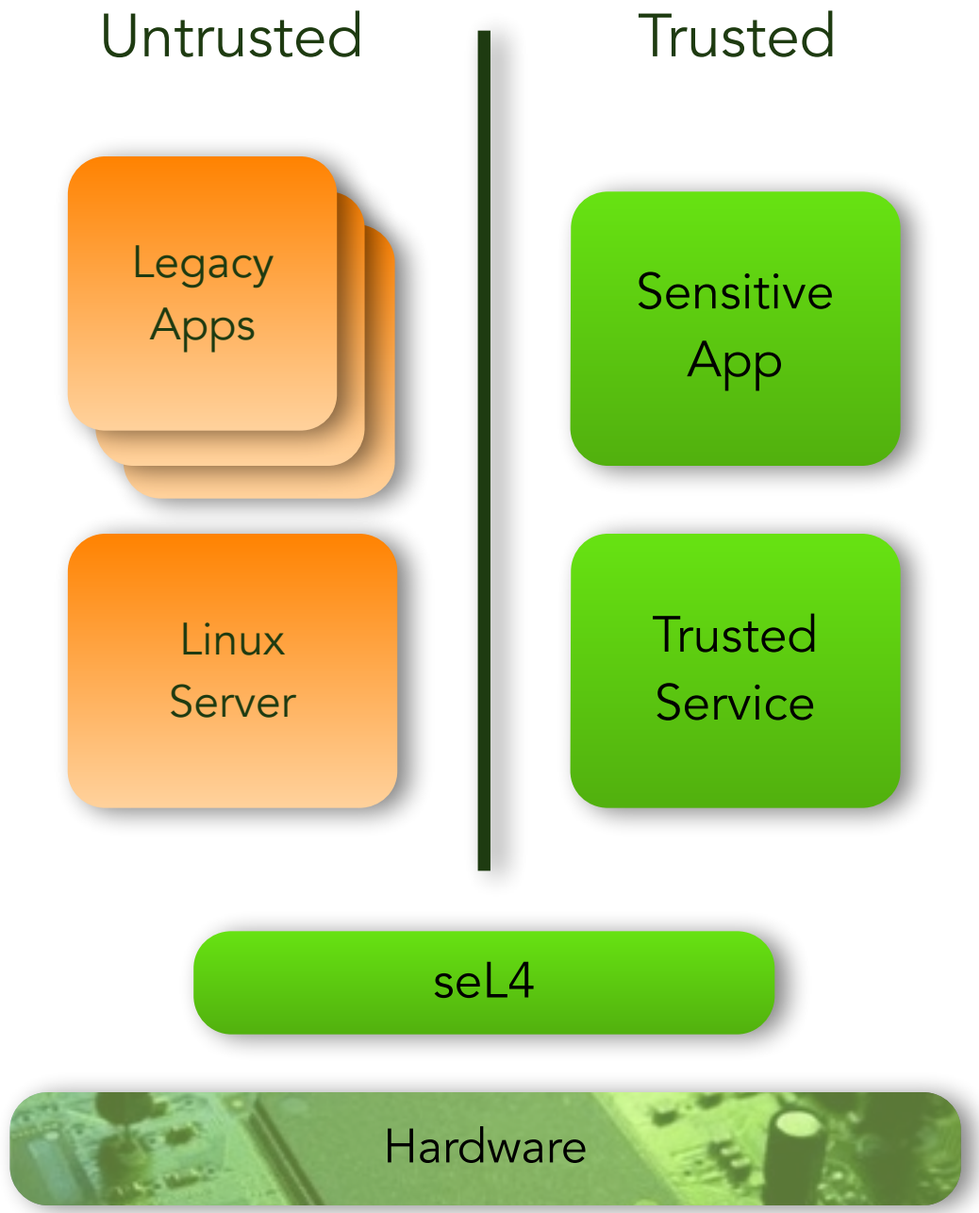
Trustworthy Computing Base

- message passing
- virtual memory
- interrupt handling
- access control

Applications

- fault isolation
- fault identification
- IP protection
- modularity

Trusted next to Untrusted



Functional Correctness Possible

NICTA

Specification

Proof

Code

Functional Correctness Possible

What

Proof

Specification

```
definition
  schedule :: unit s_monad where
  schedule ≡ do
    threads ← allActiveTCBs;
    thread ← select threads;
    switch_to_thread thread
  od
  OR switch_to_idle_thread
```

Code

Functional Correctness Possible

NICTA

What

How

Specification

```
definition
  schedule :: unit s_monad where
  schedule ≡ do
    threads ← allActiveTCBs;
    thread ← select threads;
    switch_to_thread thread
  od
  OR switch_to_idle_thread
```

Proof

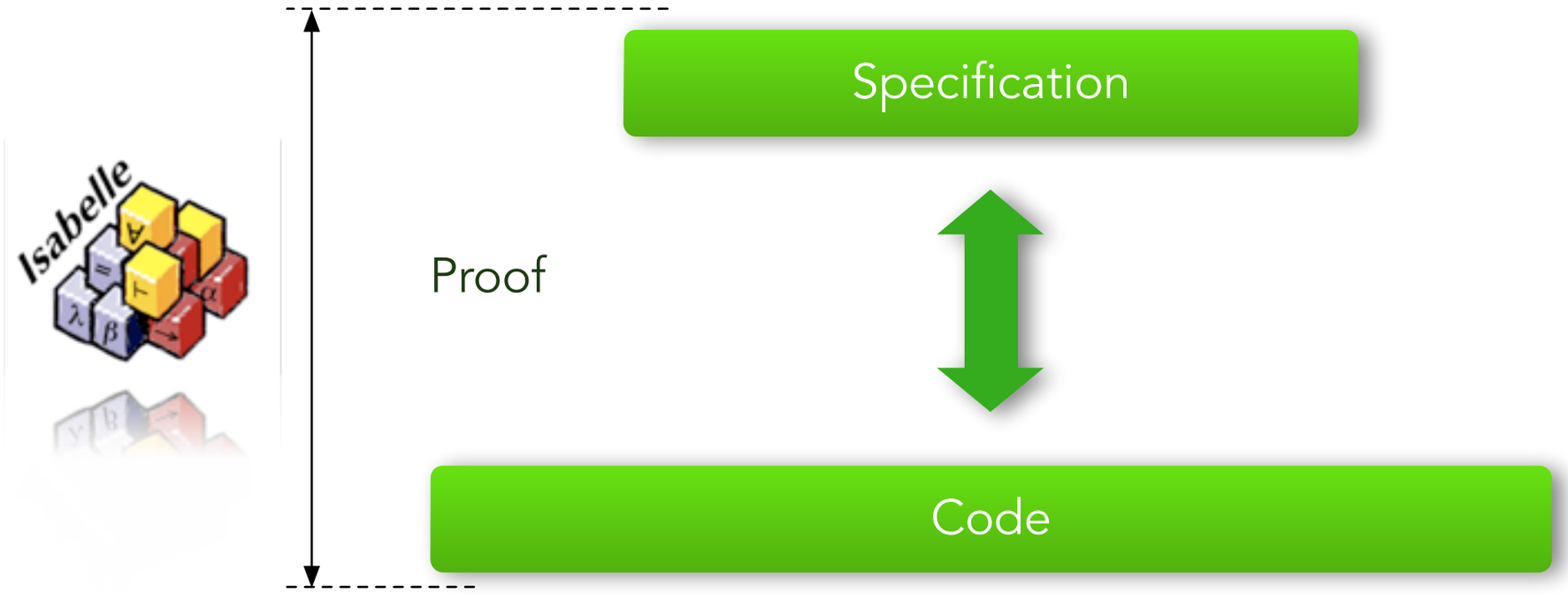
```
void
schedule(void) {
    switch ((word_t)ksSchedulerAction) {
        case (word_t)SchedulerAction_ResumeCurrentThread:
            break;

        case (word_t)SchedulerAction_ChooseNewThread:
            chooseThread();
            ksSchedulerAction = SchedulerAction_ResumeCurrentThread;
            break;

        default: /* SwitchToThread */
            switchToThread(ksSchedulerAction);
            ksSchedulerAction = SchedulerAction_ResumeCurrentThread;
            break;
    }
}

void
chooseThread(void) {
    prio_t prio;
    tcb_t *thread, *next;
```

*conditions apply



*conditions apply

NICTA

Expectation

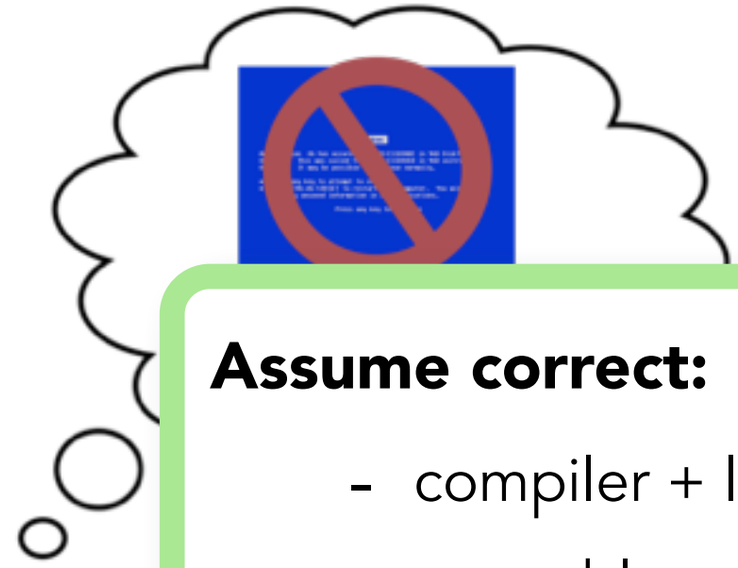
Specification

Proof

Code

Assumptions

*conditions apply



NICTA

Assume correct:

- compiler + linker (wrt. C op-sem)
- assembly code (600 loc)
- hardware (ARMv6)
- cache and TLB management
- boot code (1,200 loc)

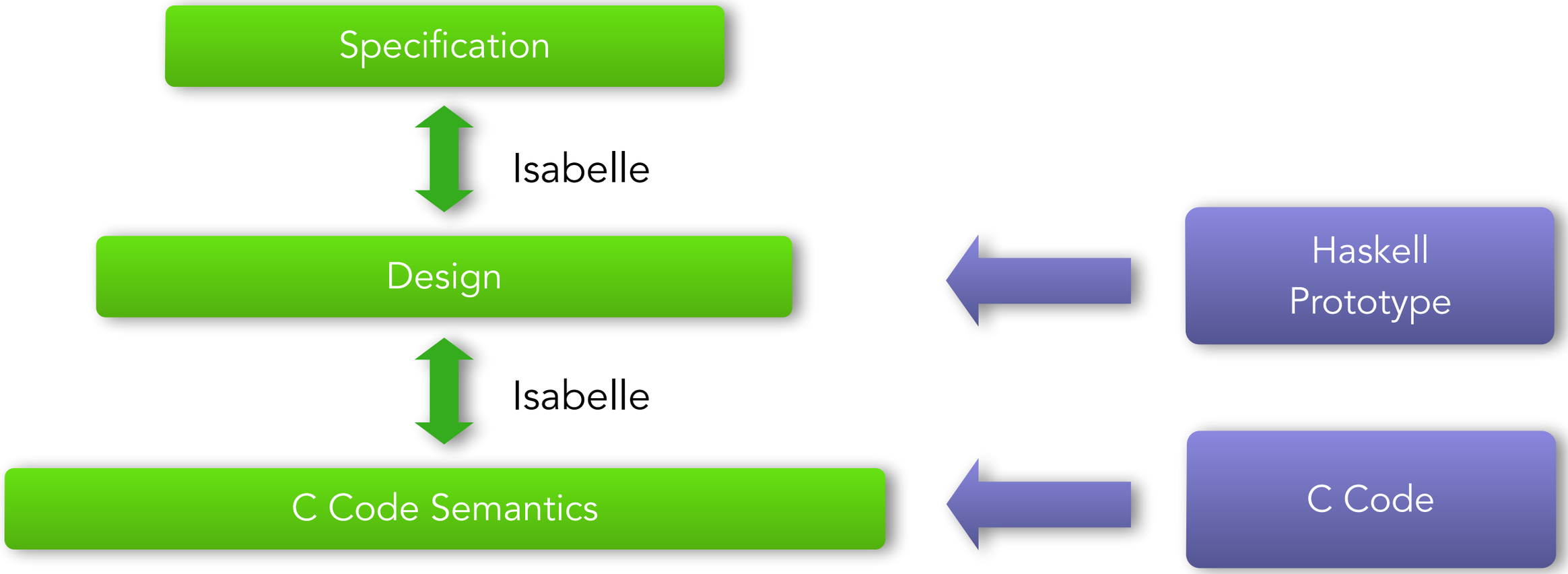
Specificatio

Proof

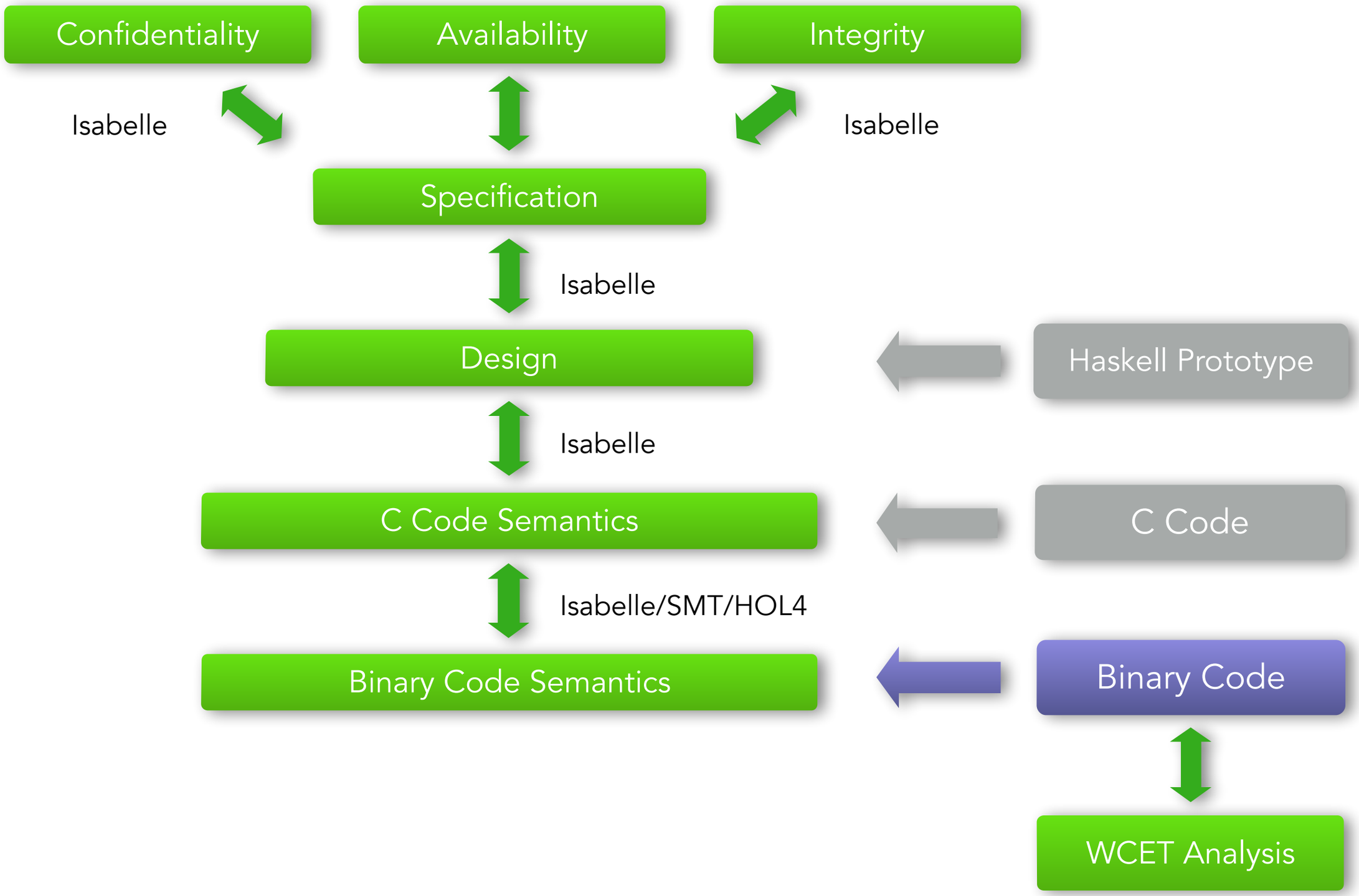
Code

Assumptions

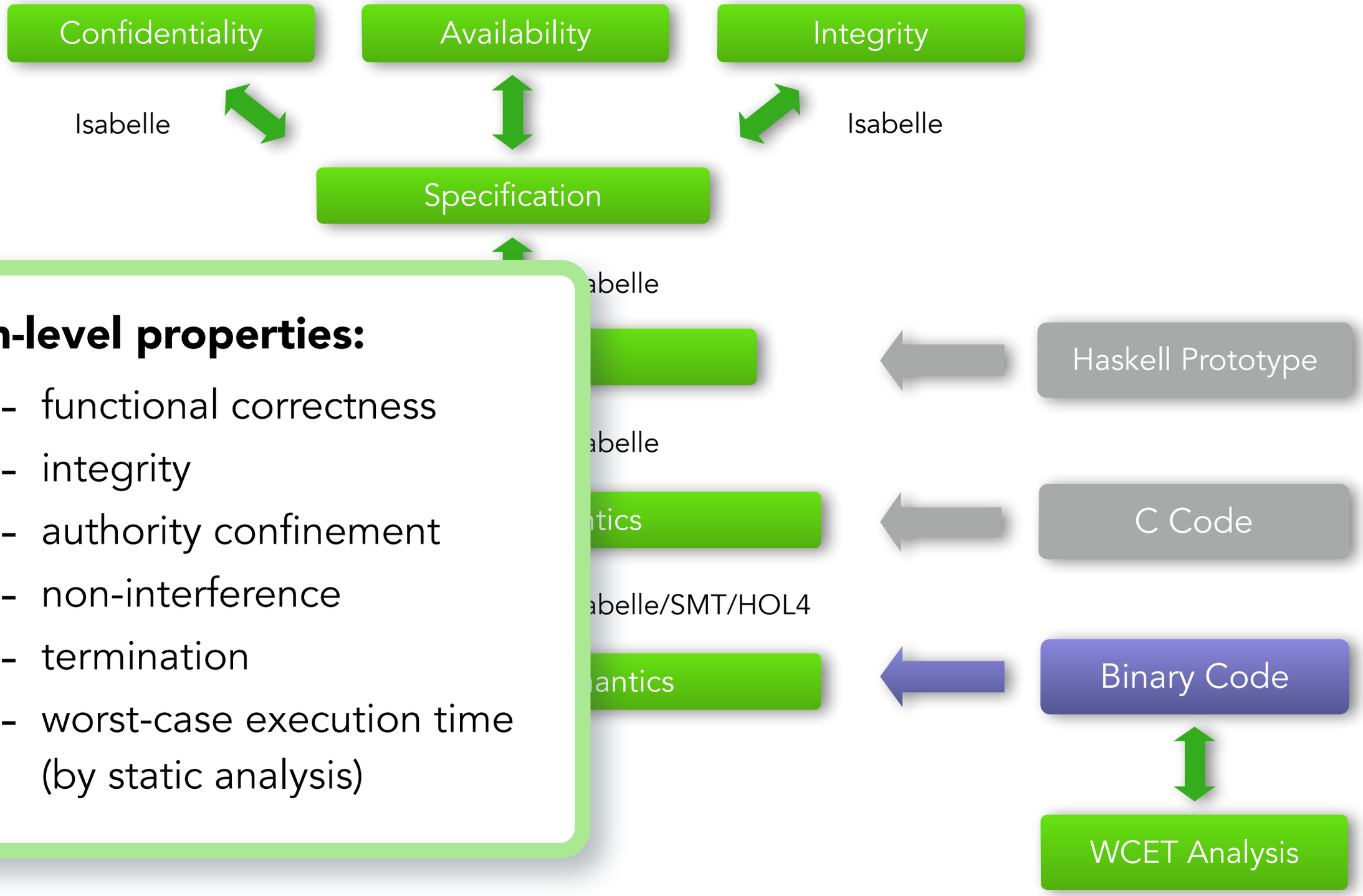
Proof Architecture [SOSP'09]



Proof Architecture Now



Proof Architecture Now



High-level properties:

- functional correctness
- integrity
- authority confinement
- non-interference
- termination
- worst-case execution time (by static analysis)

seL4: Unique Assurance

First and only general-purpose OS kernel with full functional-correctness proof – at binary level

seL4: Unique Assurance

NICTA

First and only general-purpose OS kernel with full functional-correctness proof – at binary level

First and only kernel with proof of integrity and confidentiality enforcement – at binary level

seL4: Unique Assurance

NICTA

First and only general-purpose OS kernel with full functional-correctness proof – at binary level

First and only kernel with proof of integrity and confidentiality enforcement – at binary level

World's fastest microkernel on ARM architecture

seL4: Unique Assurance

NICTA

First and only general-purpose OS kernel with full functional-correctness proof – at binary level

First and only kernel with proof of integrity and confidentiality enforcement – at binary level

World's fastest microkernel on ARM architecture

Predecessor deployed on 2 billion devices

seL4: Unique Assurance

NICTA

First and only general-purpose OS kernel with full functional-correctness proof – at binary level

First and only kernel with proof of integrity and confidentiality enforcement – at binary level

World's fastest microkernel on ARM architecture

Predecessor deployed on 2 billion devices

First and only protected-mode operating-system with complete and sound timing analysis

seL4: Unique Assurance

First and only general-purpose OS kernel with full correctness proof –

First and only kernel with proof of ... and confidentiality ...nt – at binary level

Open Source

29 July 2014

World's fastest mic... ARM architecture

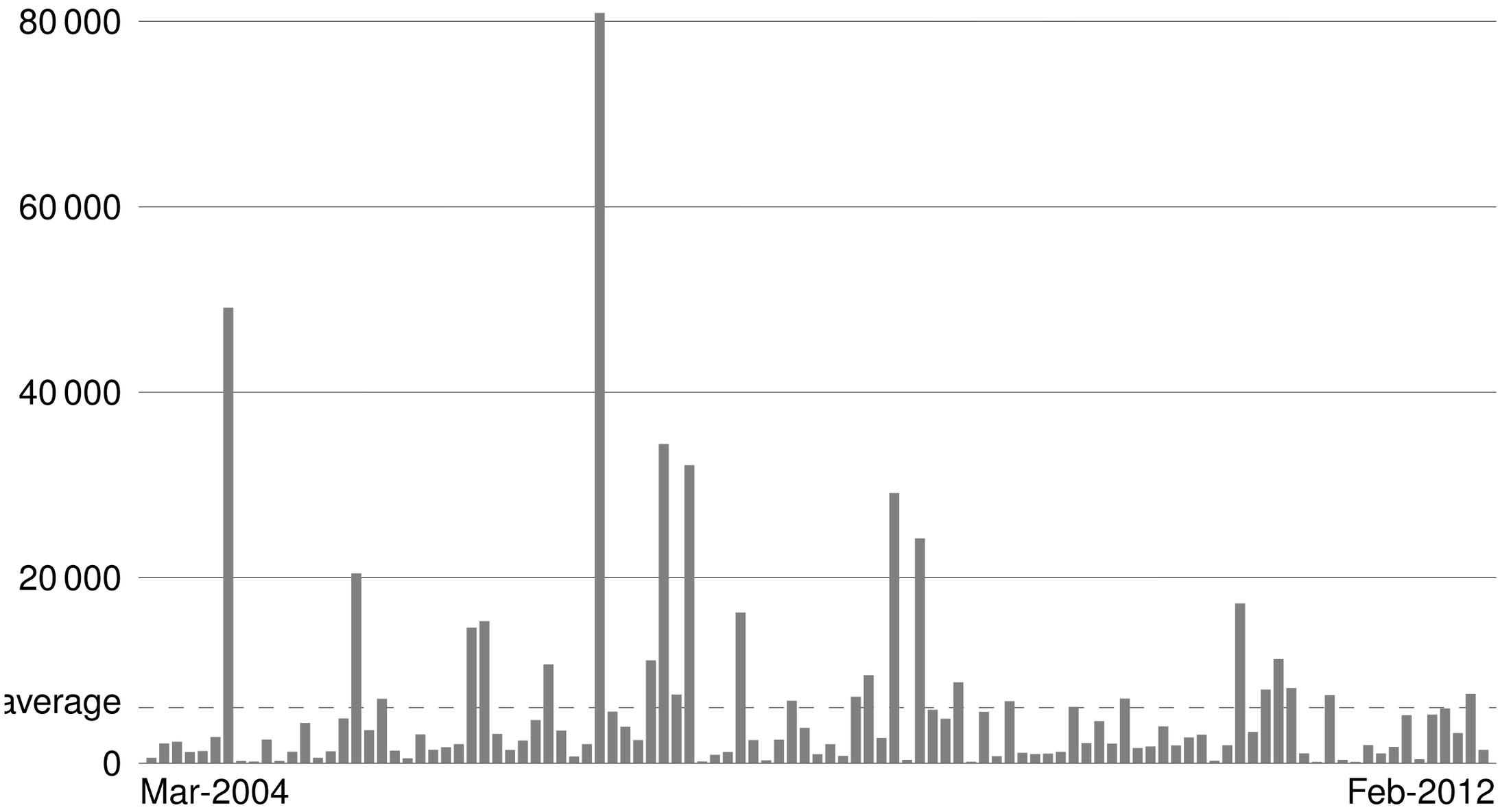
...sor deployed on 2 billion devices

First and only protected-mode operating-system with complete and sound timing analysis

Scale

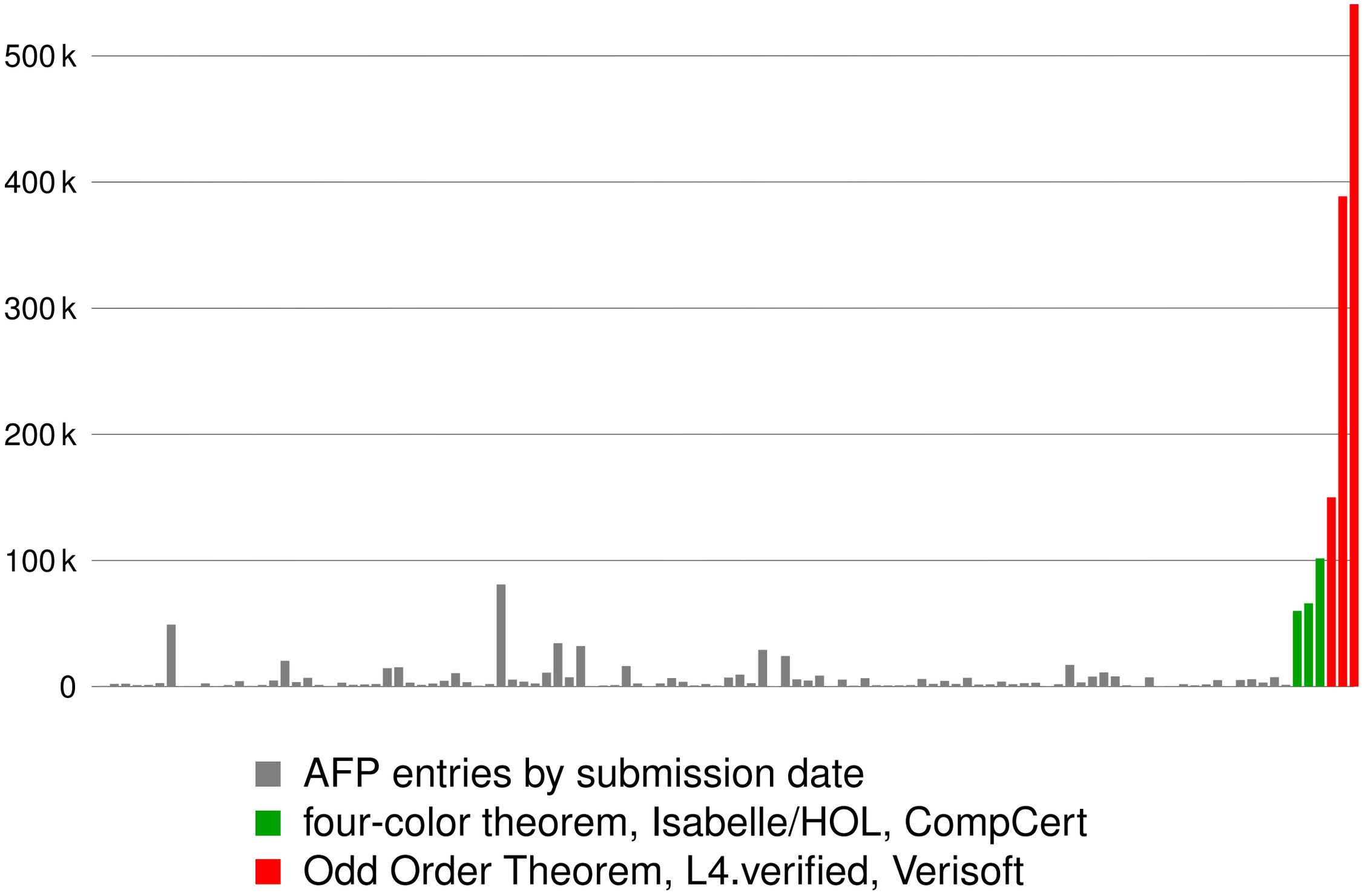
Scale

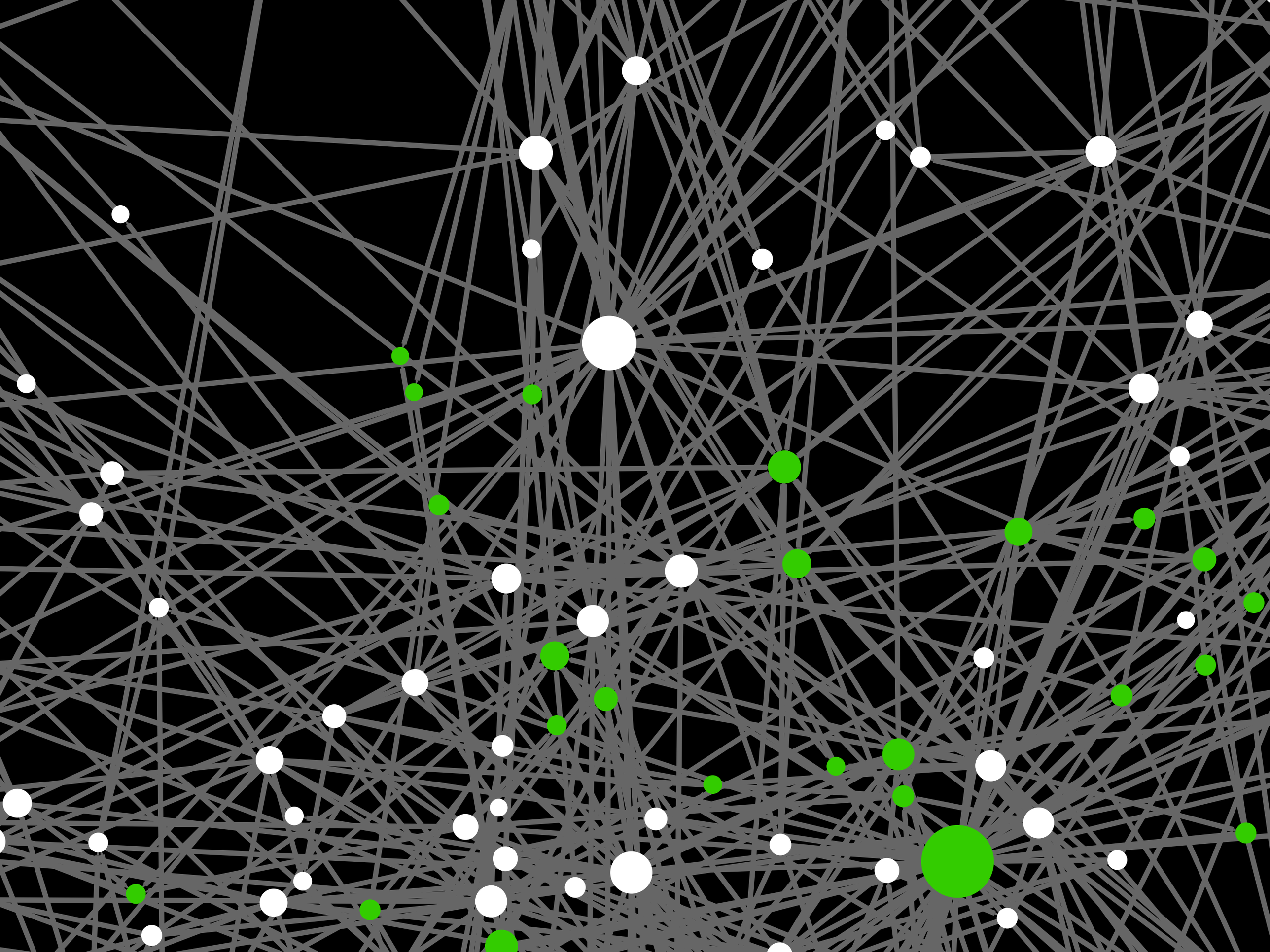
Scale



Size distribution of AFP entries in lines of proof,
sorted by submission date

Scale






seL4

Demo