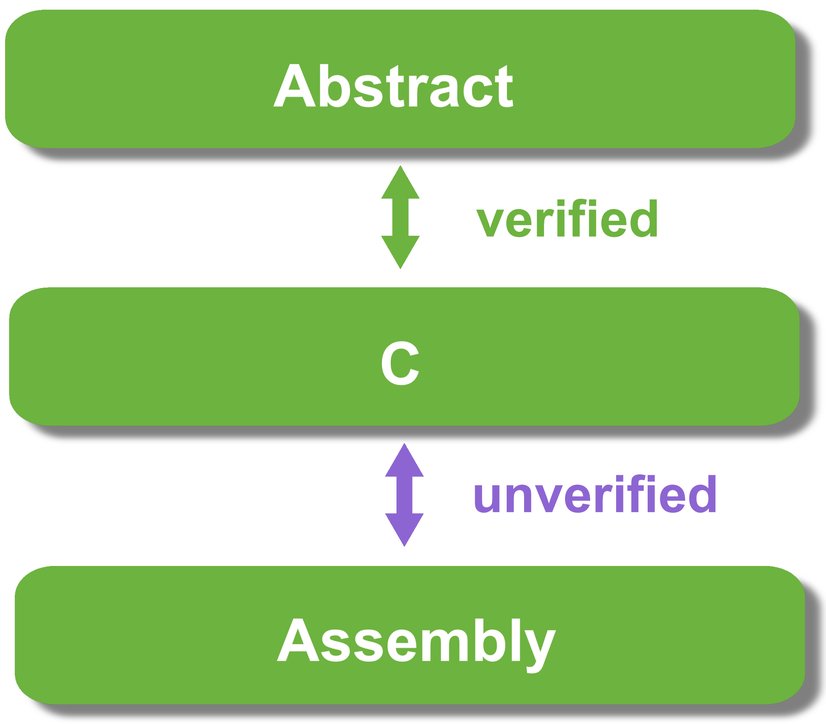
Microkernel Verification Down To Assembly

Matthew Fernandez, Gerwin Klein, Ihor Kuz

NICTA

compiling a verified kernel with a verified compiler



The Problem

seL4 is a microkernel with a formal proof of functional correctness.

This guarantees correspondence between a high level abstract specification and a low level C implementation.

The translation by the compiler of C to assembly is implicitly trusted and the prevalence of compiler bugs suggests this trust is misplaced.

Progress

✓ Compiled seL4 with CompCert

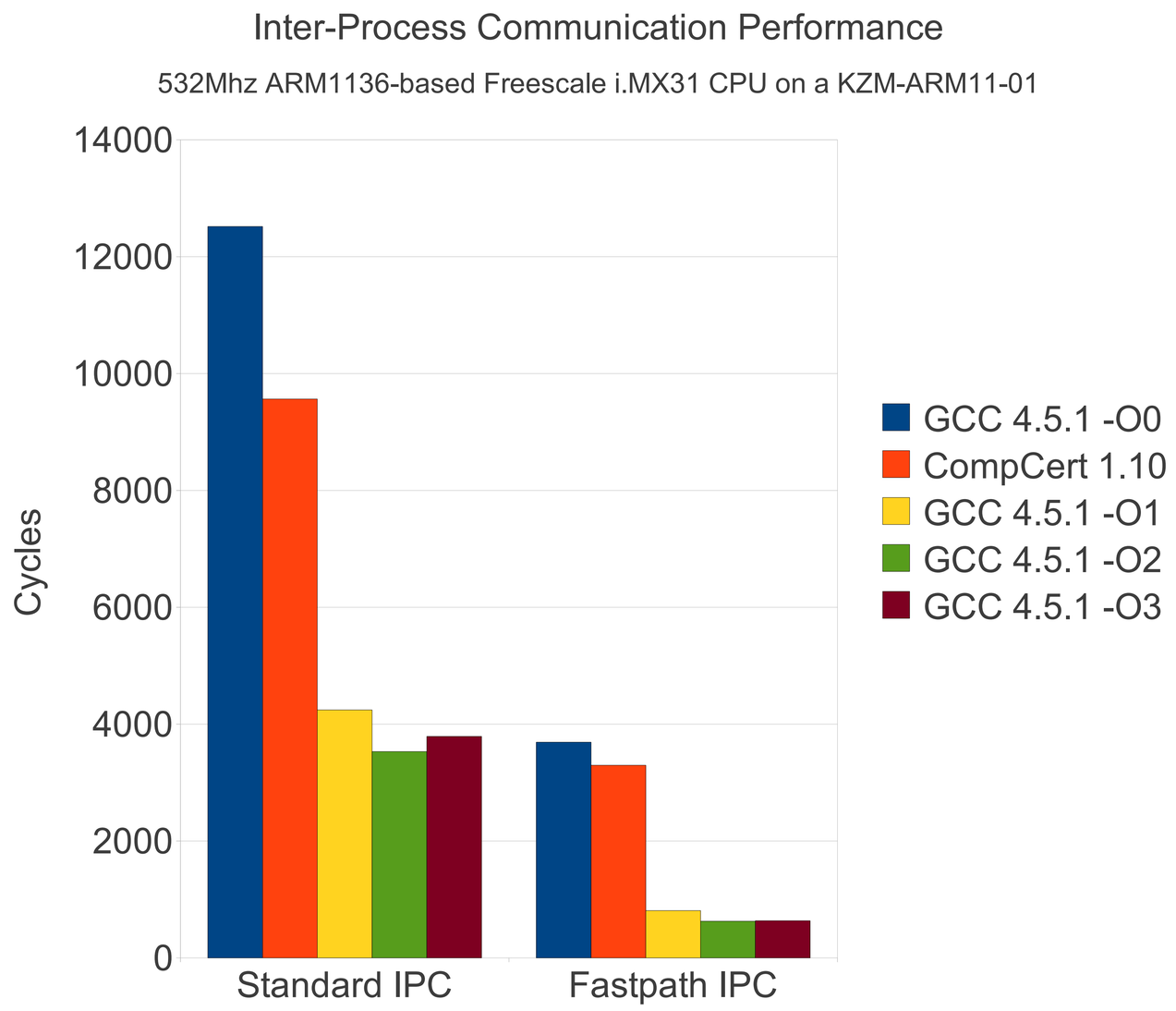
CompCert is a C compiler with a proof of correctness, developed at INRIA, France.

✓ Modifications to seL4

Approximately 500 of 9000 lines of code changed.

✓ Performance evaluation

The graph to the right depicts two scenarios, a 10 word round trip via the default IPC code path and a 4 word round trip via the optimised fastpath.



Challenges

Lacking features from CompCert

C standard ambiguity

Errors outside the proven code

GCC optimisations that hide bugs

Future Work

🕑 Proof adaptation for code changes

The modifications required to seL4 were relatively non-invasive, and we foresee no difficulties in adapting the seL4 proof.

🕑 Linking the seL4 and CompCert proofs

Preliminary investigation indicates that connecting the proofs is likely to be significantly challenging.

🕑 Extending down beyond assembly

Conclusion

We have successfully completed the first steps of this project and, in the process, exposed many hidden assumptions in seL4.

We believe this is a feasible approach to extending the guarantees of seL4, but the next steps will be challenging.

We are concurrently exploring alternative approaches to this problem in association with other researchers from NICTA/UNSW.

UNSW THE UNIVERSITY OF NEW SOUTH WALES

www.ssrg.nicta.com.au