Towards a Formally Verifiable Multiprocessor Microkernel
Michael von Tessin (NICTA and UNSW)

Userland

Kernel

Reduce parallelism by having a big lock around the whole kernel

Formal verification approach of the uniprocessor version

Reduce sharing with a multikernel approach like in Corey or Barrelfish

One isolated kernel/userland image per CPU = no sharing

Communication and resource transfer between CPUs

Resource sharing between CPUs

Progress: implemented in C and semi-formally proved

Low-level design

Reduce concurrency

Reduce proof complexity induced by concurrency

GOAL!