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

Reduce parallelism by having a big lock around the whole kernel

Reduce concurrency

Reduce proof complexity induced by concurrency

GOAL!

Reduce sharing with a multikernel approach like in Corey or Barrelfish

Userland thread obj

Kernel

CPU

Memory

One isolated kernel/userland image per CPU = no sharing

Progress: implemented in C and semi-formally proved

Formal verification approach of the uniprocessor version

Abstract Model

Concrete Model

Implementation

Userland

Kernel

CPU

Abstract Model

Concrete Model

Implementation

Isabelle/HOL

Haskell

C

C

C

Communication and resource transfer between CPUs

Resource sharing between CPUs

low-level design

Progress: implemented in C and semi-formally proved

www.nicta.com.au

From imagination to impact