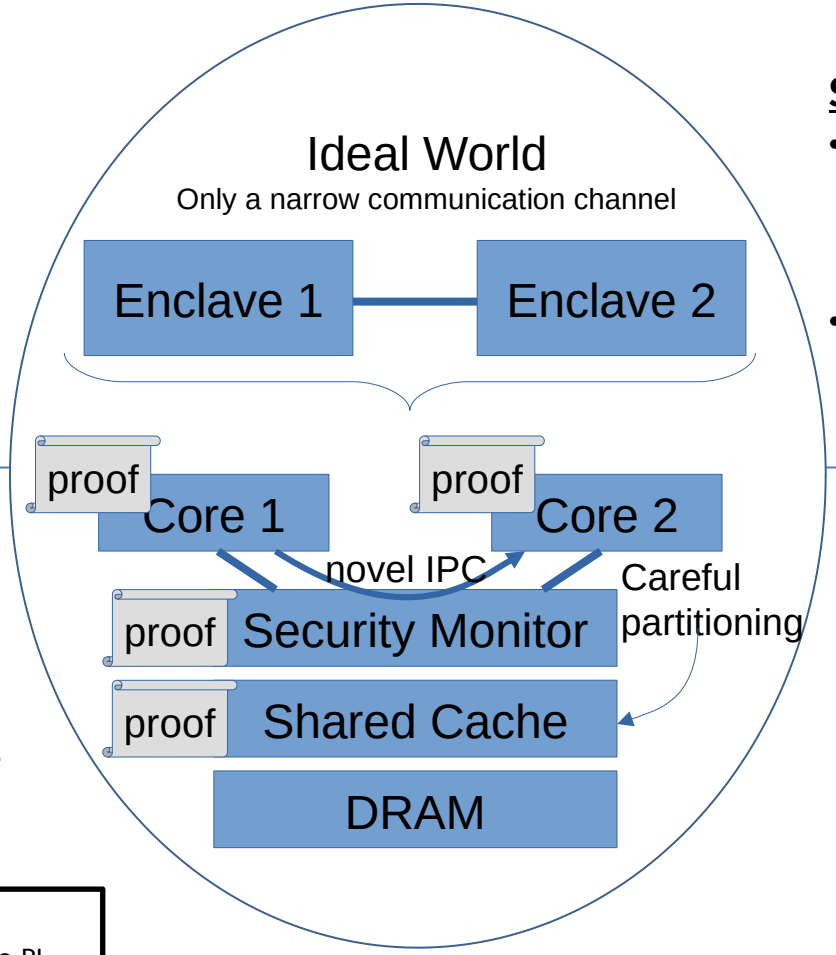
Provably Secure, Usable, and Performant Enclaves in Multicore Processors

Challenge:

- Develop strong hardware-supported isolation of software processes, with good performance and usability.
- Prove formal security properties with the Coq proof assistant.

Solution:

- New architectural primitives for enclave-to-enclave communication
- New modular proof techniques to allow separate timing-security proofs of different hardware blocks



Scientific Impact:

- Reusable design ideas for isolation (including w.r.t. timing channels) within complex, layered digital systems
- New techniques for rigorous, modular proof of timing-sensitive security properties

Broader Impact and Broader Participation:

- Release Amazon-FPGA-ready secure-processor designs (and proofs), ready to be evaluated and extended.
- Involve high-school students in security research via MIT Primes program.

#2115587, MIT,
PI Srini Devadas <devadas@csail.mit.edu>, co-PI Arvind <arvind@csail.mit.edu>, co-PI Adam Chlipala <adamc@csail.mit.edu>