Putting the C into MPC

- ORAM + MPC ⇒ oblivious arrays in MPC
- Oblivious machine
  - Code and memory in oblivious arrays
  - Execute every possible instruction in every step (constant overhead)
  - Oblivious branching
- C compiler for oblivious machine is C compiler for MPC
- Efficiency
  - Polylog overhead compared to CPU execution
  - Machine speed: a few Hz
- Private function evaluation:
  Parties learn nothing but execution time of program