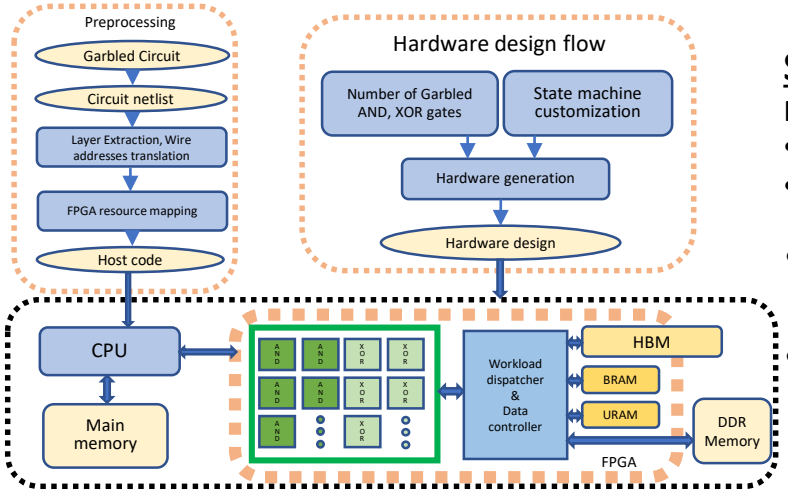
MaSSIF: Massively Scalable Secure Computation Infrastructure using FPGAs

PI: Stratis Ioannidis Co-PI: Miriam Leeser
Northeastern University

Challenge:

- Offer privacy guarantees to cloud computation
- Secure Function Evaluation (SFE) via Garbled Circuits adds computational overheads
- Exploit parallelism
  in data-oblivious fashion
- Exploit parallelism of hardware architecture and different types of memories on FPGAs in the cloud



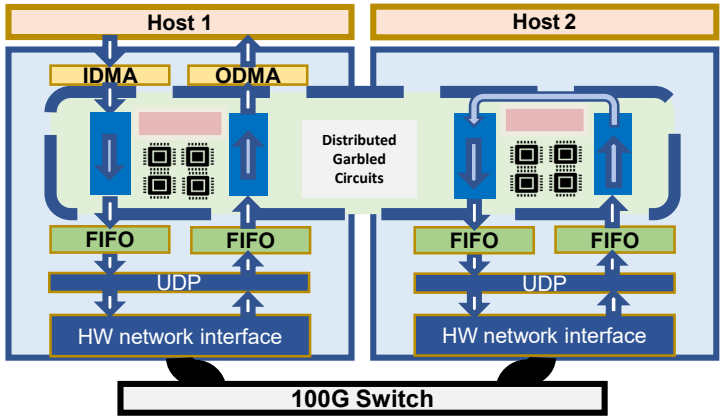
Scientific Impact:

Novel:

- Overlay architectures
- Off-chip/on-chip memory optimization
- Multi-FPGA scheduling that leverages both hardware acceleration and host parallelism
- Take advantage of the NSF funded Open Cloud Testbed (CCRI)

Solution:

- FPGAs in the Datacenter
- Key Innovations:
  - FPGA implementation of GCs
  - Re-use of hardware design via overlays
  - Multi-FPGA implementation using the Open Cloud Testbed with network attached FPGAs



Broader Impact:

- Ability to perform secure computations on the cloud at scale
- Overlays allow many different problems to be processed with very little switching time
- Privacy in ML has many potential applications, including health and wherever computation happens over sensitive data

NSF SaTC #1717213
ioannidis@ece.neu.edu
mel@coe.neu.edu