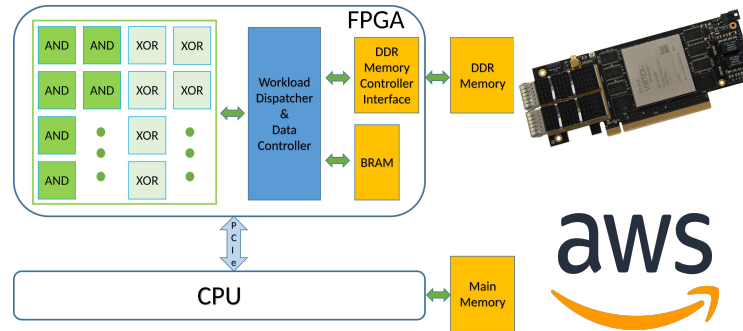# MaSSIF: Massively Scalable Secure Computation Infrastructure using FPGAs

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

Challenge:

- Offer privacy guarantees to cloud computation
- SFE via Garbled Circuits adds computational overheads
- Exploit parallelism in data-oblivious fashion

Solution:

- FPGAs in the Datacenter
- Key Innovations:
- ❏ **FPGA** implementation of GCs
- ❏ Re-use of hardware design via **overlays**
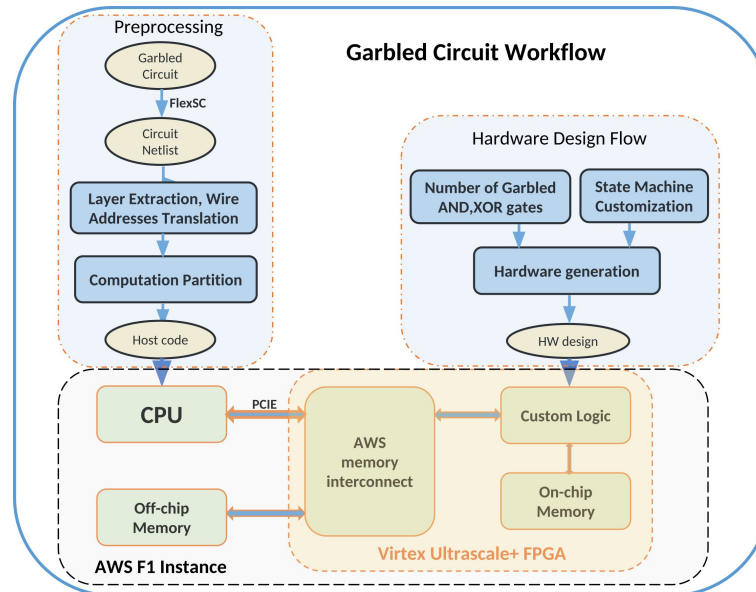- ❏ Multi-FPGA implementation

Scientific Impact:

Novel:

- Overlay architectures
- Off-chip/on-chip memory optimization
- Multi-FPGA scheduling that leverages both hardware acceleration and host parallelism

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