# 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

#### Preprocessing Garbled Circuit Workflow Garbled Circuit FlexSC Circuit Hardware Design Flow Netlist Number of Garbled State Machine Layer Extraction, Wire AND, XOR gates Customization Addresses Translation Hardware generation **Computation Partition** Host code HW design PCIE CPU Custom Logic AWS memory interconnect On-chin Off-chip Memory Memory Virtex Ultrascale+ FPGA AWS F1 Instance

#### 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

### Solution:

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





