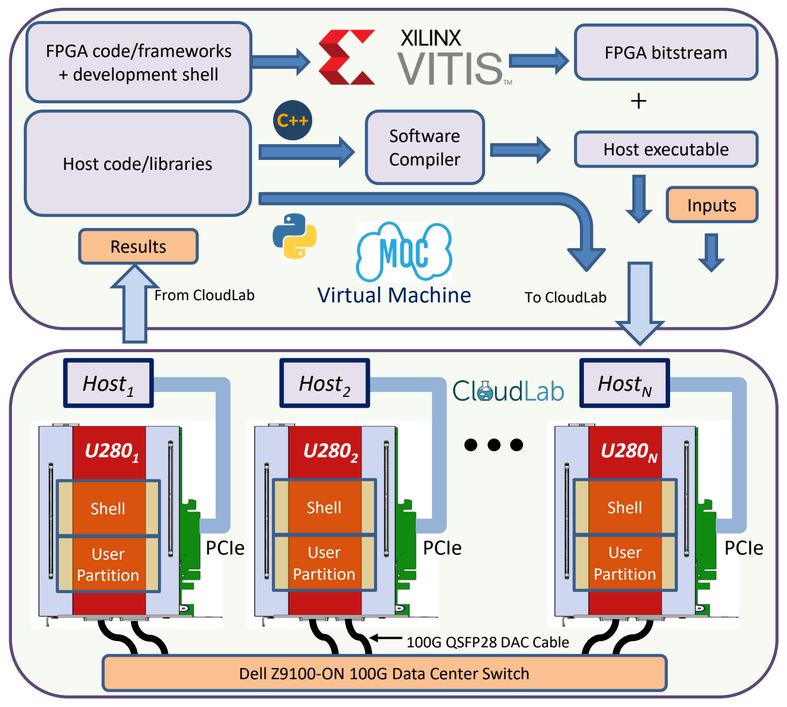
MaSSIF: Massively Scalable Secure Computation Infrastructure using FPGAs

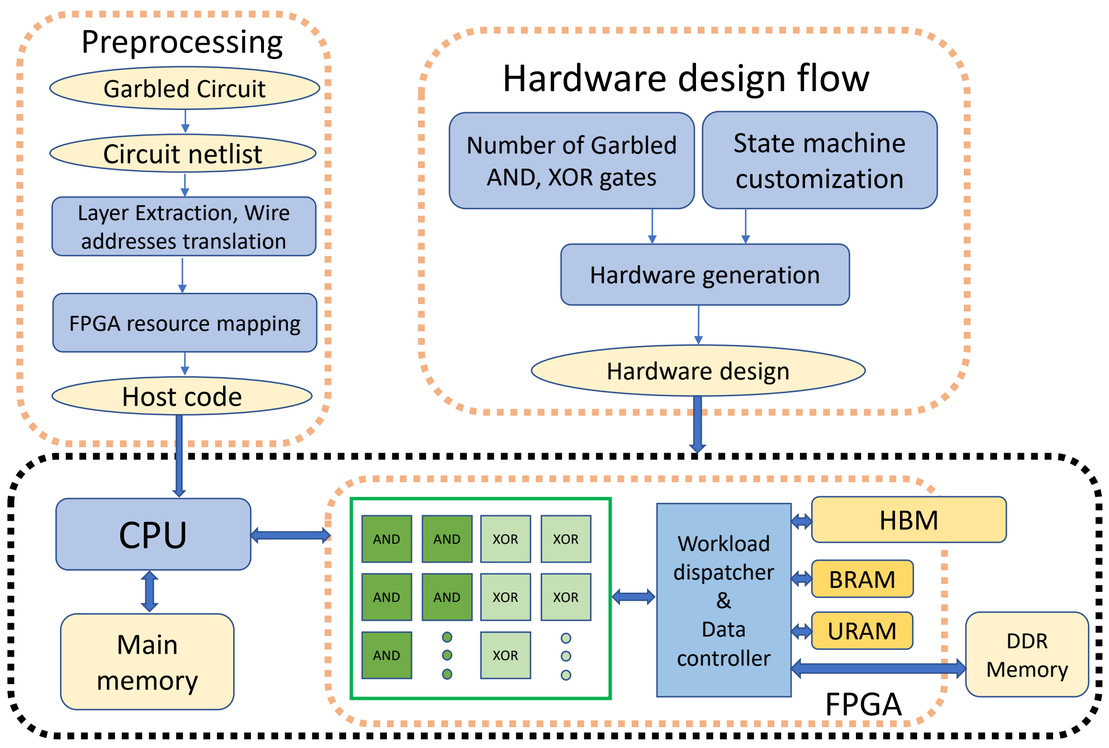
PI: Stratis Ioannidis Co-PI: Miriam Leeser
Northeastern University
NSF SaTC #1717213



Goals:

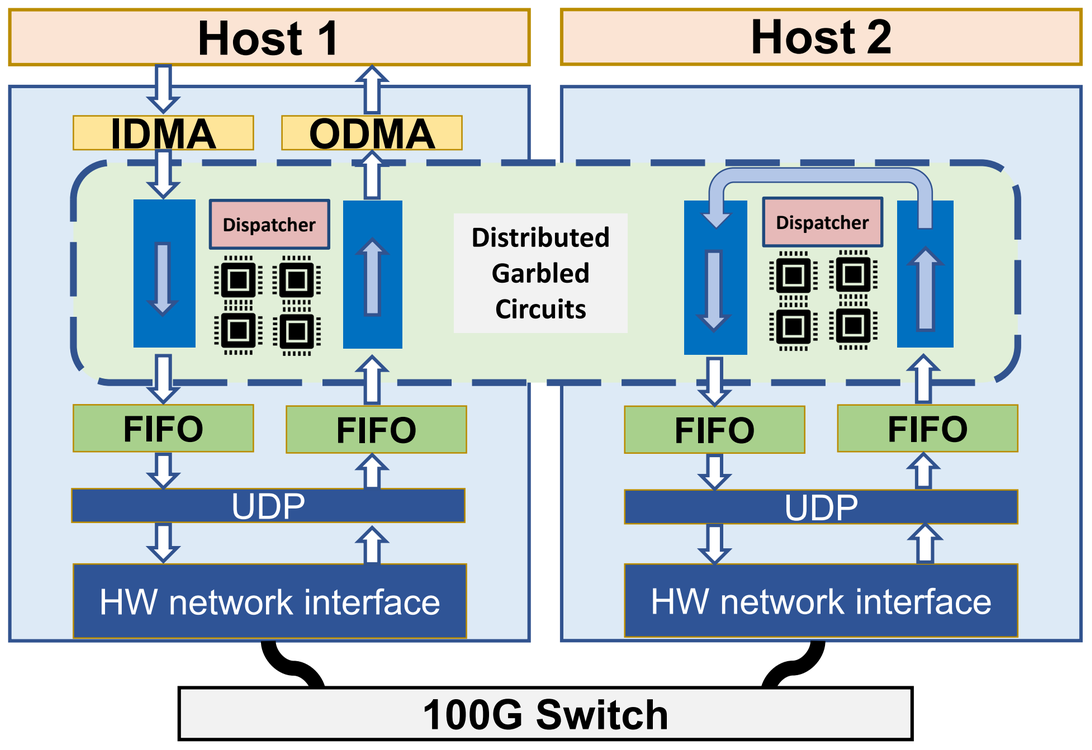
- Offer privacy guarantees to cloud computation
- SFE via Garbled Circuits adds computational overheads
- Exploit parallelism in data-oblivious fashion
- Provide improved performance
- Talke advantage of Open Cloud Testbed funded by NSF CCRI program

Garbled Circuits Workflow



- Accelerate garbled circuits on FPGA
- Explore how garbled circuits computation can be mapped to FPGA
- Include all available memories on and connected to FPGA including on chip memory (BRAM, URAM) and High Bandwidth Memory (HBM)
- Research the effects of different memory types and their combinations for Secure Function Evaluation and other applications

Multiple FPGAs



Multiple FPGA System Infrastructure

- Research non-streaming application acceleration in a distributed system environment
- Implement the design on the Open Cloud Testbed infrastructure with direct inter-FPGA communication
- Exploit efficient workload partitioning on two or more nodes
- Explore intra-FPGA and inter-FPGA parallelism to improve memory and computation throughput

Publications:

K. Huang, M. Gungor, X. Fang, S. Ioannidis, and M. Leeser, “Garbled circuits in the cloud using FPGA enabled nodes,” in IEEE High Performance Extreme Computing Conference (HPEC), Sept. 2019.
X. Fang, S. Ioannidis, and M. Leeser, “SIFO: Secure computational infrastructure using FPGA overlays,” International Journal of Reconfigurable Computing, Dec. 2019.
M. Leeser, M. Gungor, K. Huang, and S. Ioannidis, “Accelerating large garbled circuits on an FPGA-enabled cloud,” in Proc. IEEE/ACM International Workshop on Heterogeneous High-Performance Reconfigurable Computing (H2RC), Nov. 2019, pp. 19-25.
K. Huang, M. Gungor, S. Ioannidis, and M. Leeser, “Optimizing use of different types of memory for FPGAs in high performance computing,” in IEEE High Performance Extreme Computing Conference (HPEC), Sept. 2020.

- Make use of Open Cloud Testbed
- Funded by NSF CCRI Grand Program: 1925658
- Provides Xilinx Alveo U280s in CloudLab
- Eight Xilinx Alveos are currently available for users in the US
- FPGAs are directly connected to the network via 100G Ethernet connections
- Two connections per FPGA

Broader Impact:

- Ability to perform secure computations in the cloud at scale
- Privacy in ML has many potential applications, including health and wherever computation happens over sensitive data
- Investigate use of network connected FPGAs in the cloud