Enhancing FPGA Based Encryption on the Cray XD1

Joseph A. Fernando, Dennis Dalessandro, Ananth Devulapalli Ashok Krishnamurthy

{fernando, dennis, ananth, ashok}@osc.edu

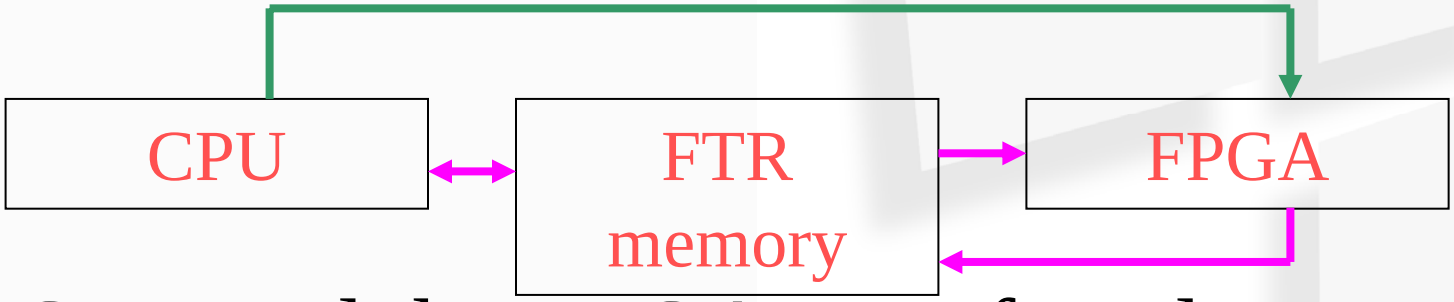
Ohio Supercomputer Center (OSC)

Springfield, Ohio 45502

Objective

- Increase Host-FPGA I/O communication bandwidth
- Develop a FPGA based I/O sub-system
- Evaluate the performance using AES Encryption

Architectural Overview



- The CPU and the FPGA transfers data through FPGA Transfer Region (FTR) memory, which is on the host.
- The source and destination pointer along with the buffer length are transferred using registers.

FTR memory based I/O

- OSC has implemented a preliminary version of a I/O interface using the FTR memory
- Objective is to use this for general purpose I/O (e.g. AES encryption)
- Use the Pull model
  - FPGA read and writes data from/to host Opteron memory
- Use burst mode to read and write
- Concurrent read and writes enabled
- Performance nearly host processor load independent
  - Minimal degradation of effective bandwidth under load

FTR memory (Cont.)

- Uses semaphores to synchronize read and write
- Use a dual port BRAM as a scratchpad
- Preliminary results are encouraging
  - Achieved a 800 MB/sec transfer rate (each way) for copy program for no load processor
  - Achieved a 785 MB/sec transfer rate under fully loaded conditions (or 2% degradation under load)
  - Achieved 1.35 GB/s if limited to one way communication
- Conducting further tests

Preliminary Results Throughput

Buffer length (bytes)	Register based Decryption (MB/s)	FTR memory based Decryption (MB/s)	Register based Encryption (MB/s)	FTR memory Based Encryption (MB/s)
256	3.2	132	3.0	160
512	3.3	237	3.1	231
1024	3.3	371	3.1	460
2048	3.3	508	3.4	587
4096	3.3	564	3.4	618
64k	3.3	568	3.44	625
1M	3.3	570	3.44	627