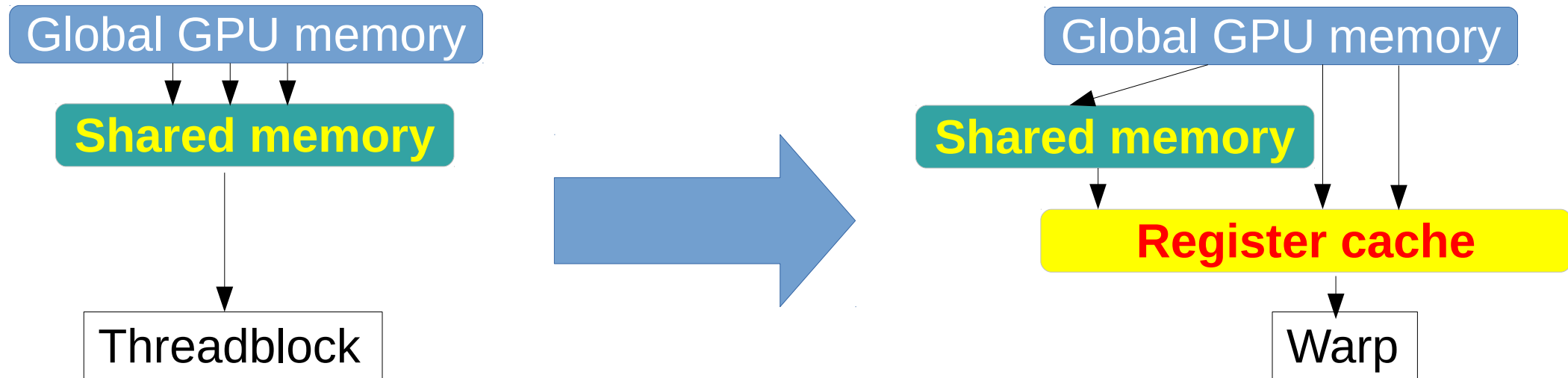


Fast Multiplication in Binary Fields on GPUs via Register Cache
Today - last session (#4) - 6:35 - 6:55pm

Register Cache

Replacing shared memory with unused registers



- Reduces (or eliminates!) shared memory traffic
- Applicable to many existing implementations

Fast Multiplication in Binary Fields on GPUs via Register Cache

Today - last session (#4) - 6:35 - 6:55pm

- Binary field multiplication: used in storage, encryption, ...



- Register Cache: 50% performance boost