SHAKE128 GPU 구현

정보컴퓨터공학과 권혁동

한성대학교 HANSUNG UNIVERSITY

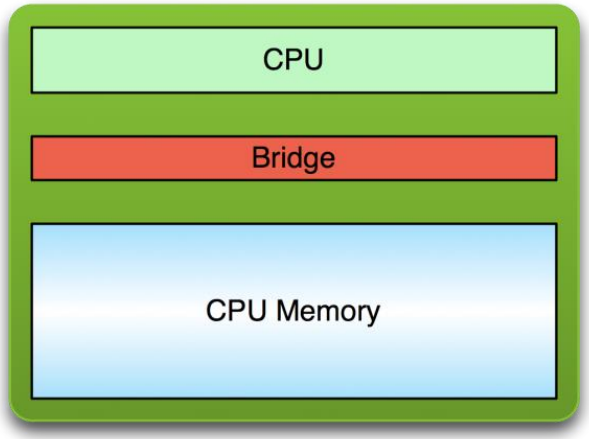
CryptoCraft LAB
https://crypto.modoo.at

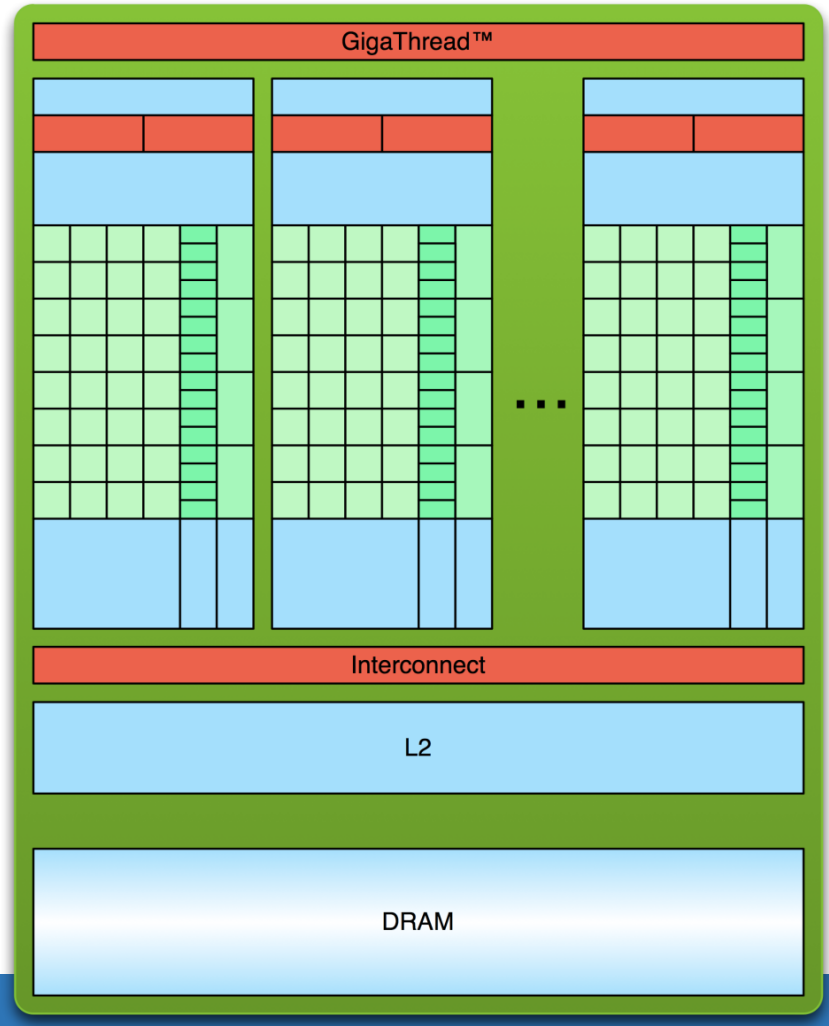
Contents

CryptoCraft LAB

GPU 프로그래밍

- 2000년대 초반 이후로 CPU보다 GPU의 성능이 비약적으로 발전
- GPU는 **병렬 처리에 유리**함
- GPU 상에서 연산을 위해서는 복사가 필요
  - 연산 전: CPU -> GPU
  - 연산 후: GPU -> CPU



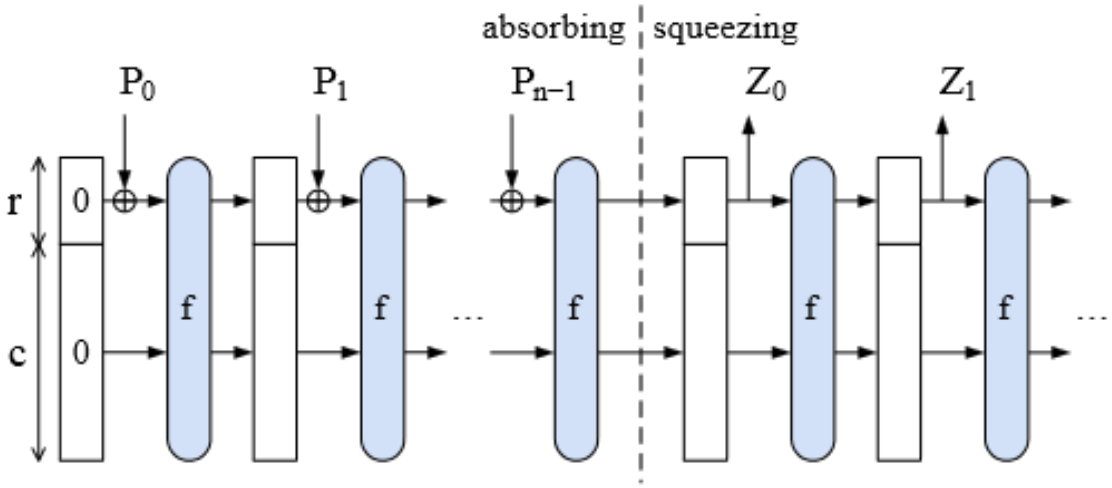


GPU 프로그래밍

- Host와 Device로 분류하여 호칭
  - CPU: Host
  - GPU: Device
- 일반적으로 함수는 CPU만 실행, 호출 권한을 지님
- **__global__** 키워드가 있는 함수는 Device의 실행 권한을 제공
- Host에서 Device로 매개변수를 이동시켜야 함
  - cudaMalloc()
  - cudaMallocHost()
  - cudaMemcpy()
  - cudaFree()

SHAKE128

- SHA3 해시 알고리즘 중 하나
- 고정 출력길이: SHA3-224, SHA3-256, SHA3-384, SHA3-512
- 가변 출력길이: SHAKE-128, SHAKE-256
- **Keccak 알고리즘** 적용
  - 2012년 SHA-3 경진 우승
  - 2015년 표준 지정
- 스펀지 구조 사용



구현

- 코드 및 동작은 세미나 영상에서 확인

결론

- GPU 프로그래밍을 통해 SHAKE128을 구현
- 블록, 스레드 수에 따라 동작 시간이 달라지는 것을 확인 가능
- 후속 과제
  - PTX 어셈블리를 통해 추가적인 최적화 구현
  - Coarse grain이 아닌, Fine grain 구현 시도