CUDA 를 이용한 DES 구현

김주호*, 박능수*
*건국대학교 컴퓨터공학과
e-mail : juho0719@naver.com

Implementation of DES Algorithm using CUDA

Juho Kim*, Neungsoo Park*
*Dept. of Computer Science and Engineering, Konkuk University

요 약

GPU 를 이용하여 병렬 처리 연산을 하는 연구는 활발히 진행되고 있고, 이미 많은 곳에서 사용되고 있다. 본 논문에서는 엔비디아에서 개발한 CUDA 를 사용하여 DES 알고리즘을 고속으로 구현하기 위해 CUDA overlapping 을 이용했다. 이것은 GPU 에서 연산을 하는 동시에 연산 결과를 바로 Host 로 보내어 연산시간과 전송시간을 Overlap 하여 시간을 더 단축 하도록 하는 구현방법이다. 그 결과 Overlap 하기 전보다 약 30%의 성능향상을 확인 할 수 있었다. 향후 DES 뿐만 아니라 3DES, AES, SEED 등 여러 암호화 알고리즘들도 적용할 예정이다.

1. 서론

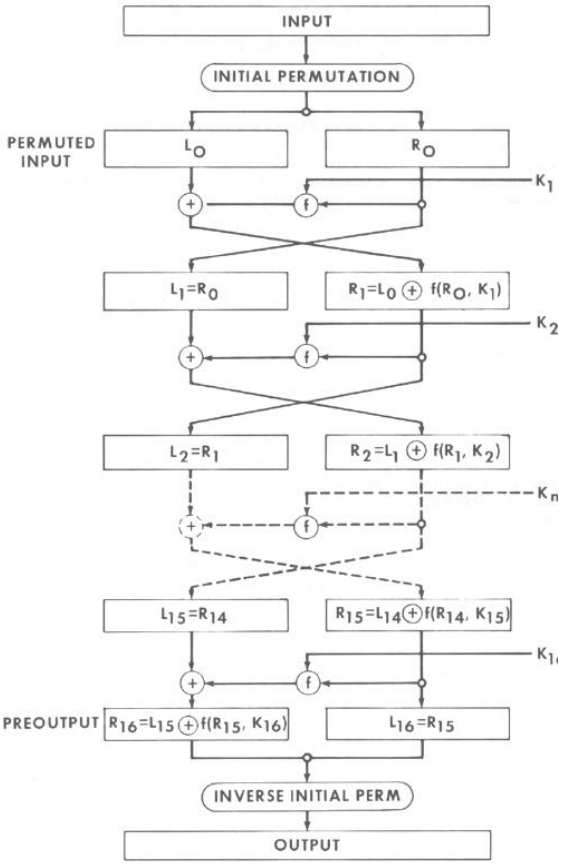
최근 GPGPU(General Purposed Graphic Processor Unit)에 대한 연구가 활발히 진행되고 있다. GPGPU 란 그동안 그래픽 처리용도로만 사용되었던 GPU 를 사용하여 CPU 의 일들을 처리하도록 하는 기술이다. 하지만 GPGPU 기술을 이용하여 개발하는 데에는 그래픽스에 대한 전문지식이 많이 요구되어 사람들이 사용을 하지 못했다. 그러나 엔비디아에서 CUDA 컴퓨팅 모델을 발표하면서 사람들이 쉽게 사용할 수 있도록 개발되었고, CUDA 를 이용하여 DES 알고리즘을 보다 빠르게 구현하는 시도가 있었다[1]. 본 연구에서는 Communication 과 Computation 을 Overlap 할 수 있는 기술을 DES 를 CUDA 에서 구현하는데 적용하여 성능을 향상시키고자 한다.

2. DES Algorithm

DES 는 Data Encryption Standard 의 약자로 블록 암호화 방식이다. 암호키와 복호키가 같은 대칭키 암호로 1977 년 미국 표준 암호 알고리즘으로 채택되어 여러 분야에서 사용되고 있다.[2]

DES 는 64 비트의 평문이 16 라운드를 거쳐 64 비트 암호문이 나온다.

64 비트의 평문 메시지 블록을 받아 서브키들과의 연산을 통해 암호화가 진행된다. 그 이후 초기 재배열로 전치가 이루어 지고, 평문 메시지를 좌, 우 32 비트씩 나눈다. F 함수를 Feistel 알고리즘으로 반복 처리하고, 생성된 서브키를 이용하여 S 박스를 거치고, 이를 16 라운드에 걸쳐 반복 실행하면, 암호문이 생성된다. (그림 1)

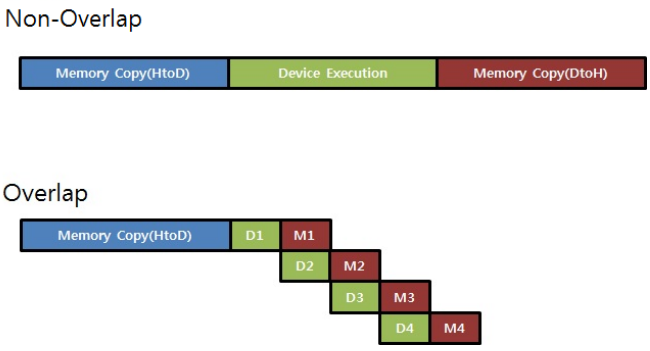


(그림 1) DES 암호화 진행과정

3. CUDA 를 이용한 DES 구현

CUDA 는 cudaMemcpy() 또는 cudaMemcpyAsync()를 통해 호스트 메모리에 있는 데이터를 디바이스에 복사하고, 디바이스에서는 그 복사한 데이터를 실행한다. 그리고 그 결과값을 다시 호스트에 복사해 주는

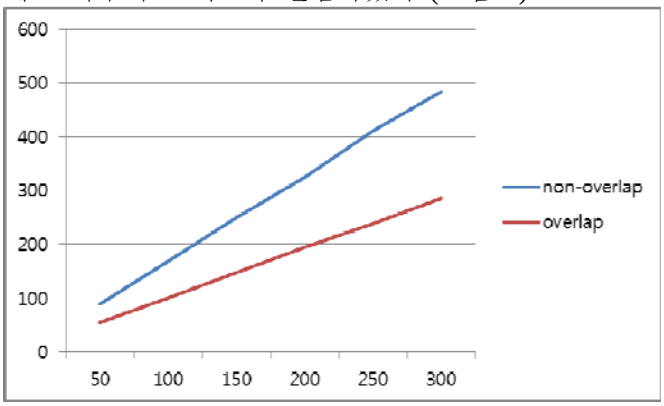
것이 CUDA 프로그램의 일반적인 단계이다. 하지만 Compute Capability 1.1 이상 버전부터는 디바이스에서 연산을 하는 동시에 호스트로 데이터도 보낼 수가 있다. 이점을 이용하여 디바이스에서 데이터를 실행하고, 그 결과값을 호스트에 전달해주는 작업을 overlap 하였다. (그림 2)



(그림 2) CUDA Overlapping 구현 방식

4. 실험결과

실험은 GeForce GTX260 이 있는 데스크탑에서 실시했다. 4 개의 Stream 을 이용했고, 데이터는 균등하게 4 개로 나누어 보내도록 실험하였다. (그림 3)



(그림 3) 성능 측정 그래프

x 축은 암호화한 데이터 용량을 나타내고, y 축은 시간을 나타낸다. 그림 3 을 보면 non-overlaping 하게 처리한 것 보다 약 30%이상 성능 향상이 이루어 진 것을 확인했다.

5. 결론 및 향후 계획

CPU 에서 처리한 것보다 GPU 에서 병렬처리한 것이 고속으로 암호화 알고리즘을 구현할 수 있었다. 본 논문은 그뿐만 아니라 연산과 메모리 복사를 Overlap 을 하여 DES 알고리즘을 구현, 30%의 속도향상을 기록했다. 향후 DES 뿐만 아니라 3DES, AES, SEED 등 여러 암호화 알고리즘에도 적용시켜 실험을 예정이고, 이를 비교 분석할 예정이다.

참고문헌

[1] 엄용진, 조용국. “GPU 용 연산 라이브러리 CUDA 를 이용한 블록암호 고속 구현” , 한국정보보호학회, 정보보호학회논문지 18(3), 2008. 6.

[2] William M. Daley, Raymond G. Kammer, “Data Encryption Standard(DES)”, FIPS PUB 46-3, 1999. 8.

[3] Steve Rennich, “CUDA C/C++ Streams and Concurrency”, NVIDIA