OpenMP를 활용한 LSH DRBG 병렬 최적 구현

권혁동 * 안규황 * 서화정 *†
* 한성대학교 대학원 정보시스템공학과

요 약

● 미국 국립표준연구소(NIST)에서 권고하는 결정론적 난수 발생기(DRBG)를 구현

● 병렬화 적용이 가능한 부분을 병렬처리로 변경하여 성능 향상을 도모

연구 목적

● SHA-2, SHA-3가 적용된 DRBG를 국내 표준에 적합하도록 LSH를 이용하여 이식 구현

● DRBG의 내부 구조 중 반복적이지만 서로 독립적인 연산 부분을 병렬화하여 성능을 향상시키고자 함

연구 방법

● 데이터 병렬화와 태스크 병렬화 두 기법을 사용하여 기존 구조와 동작 속도를 비교

```
Algorithm
1. read test vectors
2. loop count = number of hash output types
3. operate OpenMP to for loop
4. For i = 1 to loop count
   4.1 DRBG using hash[i] type
   4.2 write DRBG result
   4.3 waiting until other processing finished
5. DRBG finished
```

Fig. 1. (left) 데이터 병렬화가 적용된 의사 코드

```
Algorithm
1. len = ceil (output bits from parameter / hash bits)
2.1 If hash bits is 224 or 256
      seed bits = 440
2.2 If hash bits is 384 or 512
      seed bits = 888
3. data = state V from parameter
4. operate OpenMP to for loop
5. For i = 1 to len
   5.1 output[i] = Hash(data)
   5.2 data = (data + 1) mod 2^seed bits
   5.3 waiting until other processing finished
6. final output = (output[1] || … || output[n]) mod 2^output bits
```

Fig. 2. (right) 태스크 병렬화가 적용된 내부 출력 생성 함수 의사 코드

연구 결과

● 데이터 병렬화가 적용된 구조는 기존의 구조보다 약 2.71배의 성능 향상을 보임

	평균수행시간(ms)	cpb
대조군	73	491
병렬화	27	181

Table. 1. 데이터 병렬화 성능 비교

● 태스크 병렬화가 적용된 구조는 기존의 구조보다 약 2.04배의 성능 하락을 보이나 DRBG의 출력 길이가 증가함에 따라 조건부 성능 향상을 꾀할 수 있음

	평균수행시간(ms)	cpb
대조군	73	491
병렬화	149	1001

Table. 2. 태스크 병렬화 성능 비교

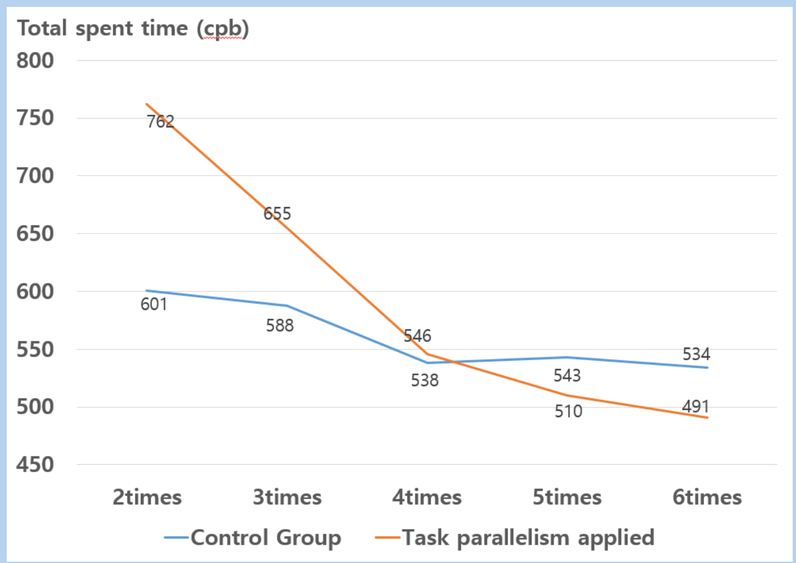

Fig. 3. 출력 길이 별 성능 비교

결 론

● 데이터 병렬화가 적용된 DRBG는 기존 구조보다 성능 향상을 보임

● 이를 활용하여 동시에 다른 규격의 DRBG 출력 값을 확보하는 것이 가능함

● 태스크 병렬화가 적용된 DRBG는 출력 규격에 일치하지는 않지만 조건부 성능 향상이 가능함

Github: https://github.com/korLethean/DRBG_with_MP