OpenMP를 활용한 LSH DRBG 병렬 최적 구현

2019. 02. 11. 영남지부 학술대회

한성대학교 IT응용시스템공학과
권혁동 안규황 권용빈 서화정

HSU HANSUNG UNIVERSITY

목차

HSU
HANSUNG
UNIVERSITY

1. DRBG 소개

1.1 DRBG(Deterministic Random Bit Generator)

- 컴퓨터에서 난수 생성은 함수 연산을 통해 이루어짐
- 따라서 완전 난수 생성은 매우 까다로움
- 입력에 따라 값이 종속되는 의사 난수를 사용
- 값이 정해져 있기에 결정론적 난수 생성기라 칭함
- NIST SP 800-90a 표준 문서 공표

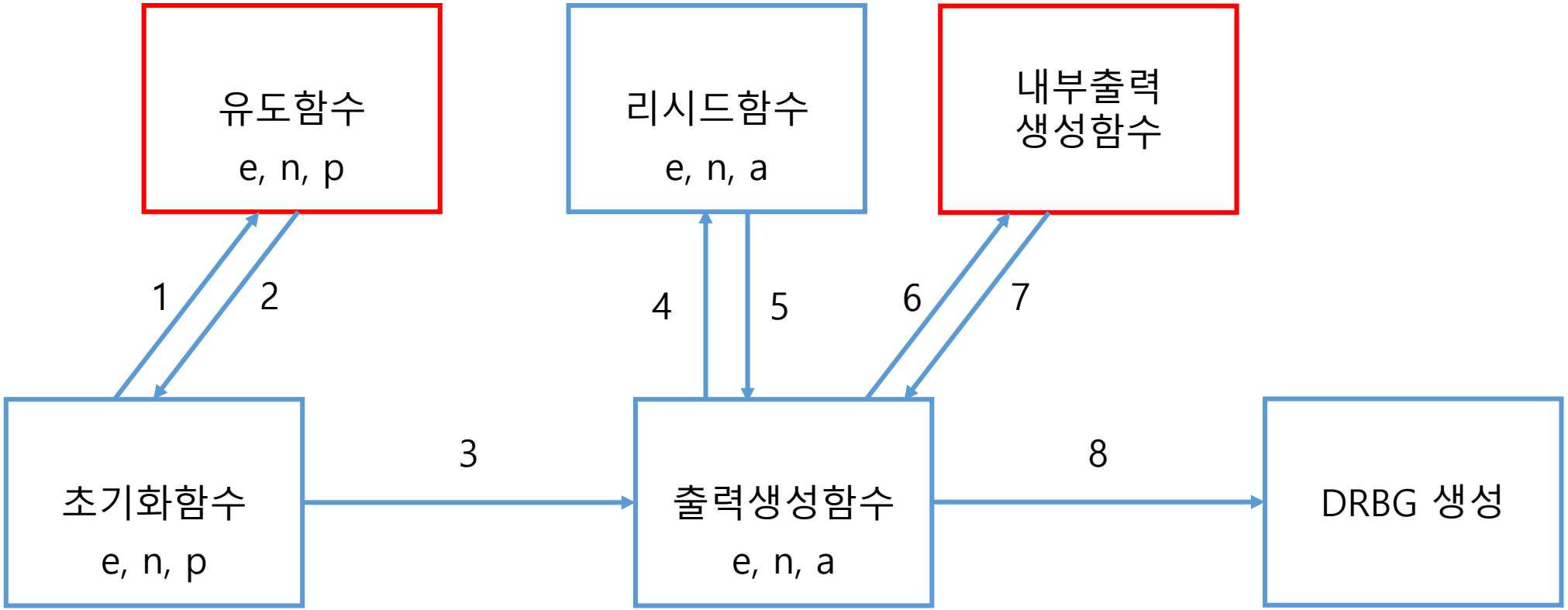
HSU HANSUNG UNIVERSITY

1.2 DRBG 입력

- 엔트로피(entropy): 측정된 무질서한 값
- 논스(nonce): 무작위 생성 값
- 개별화문자열(personalization_string): 추가적인 입력
- 추가입력(additional_input):추가적인 입력

1.3 DRBG 구조

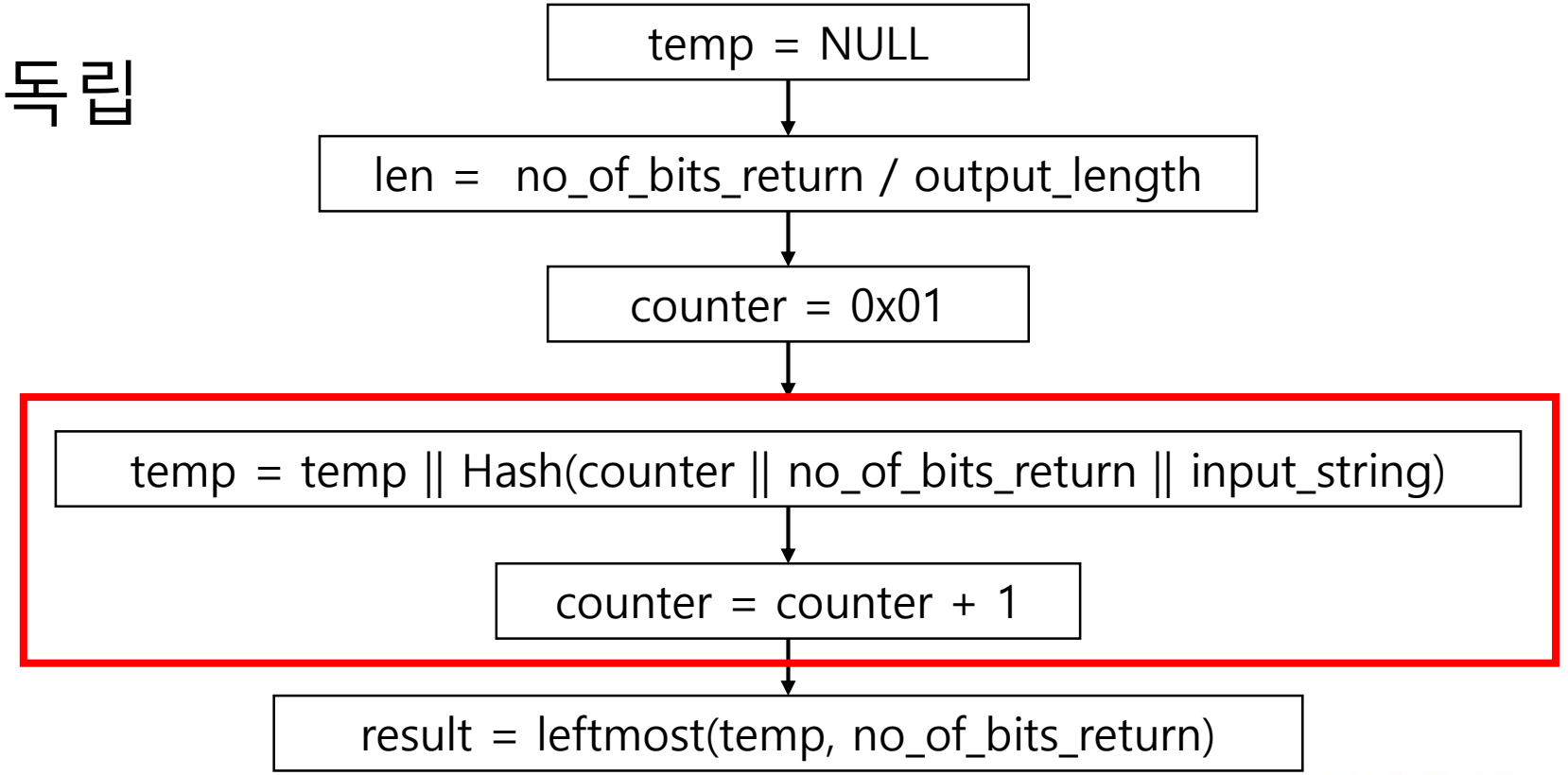
* e: 엔트로피, n: 논스, p: 개별화문자열, a: 추가입력



HSU HANSUNG UNIVERSITY

1.3 DRBG 유도함수 구조

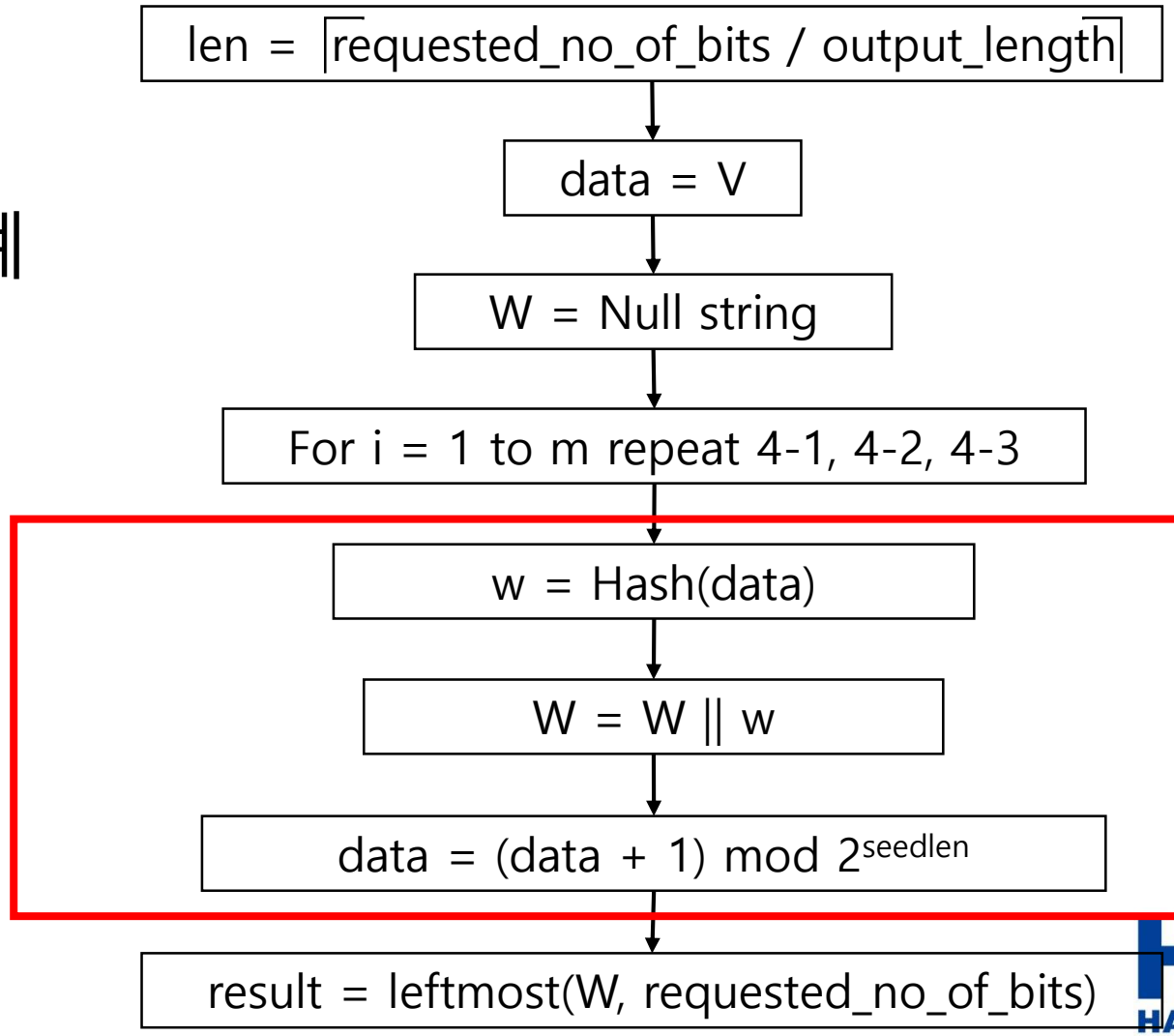
- 최대 3회까지 반복
- temp 값은 서로 독립



HSU HANSUNG UNIVERSITY

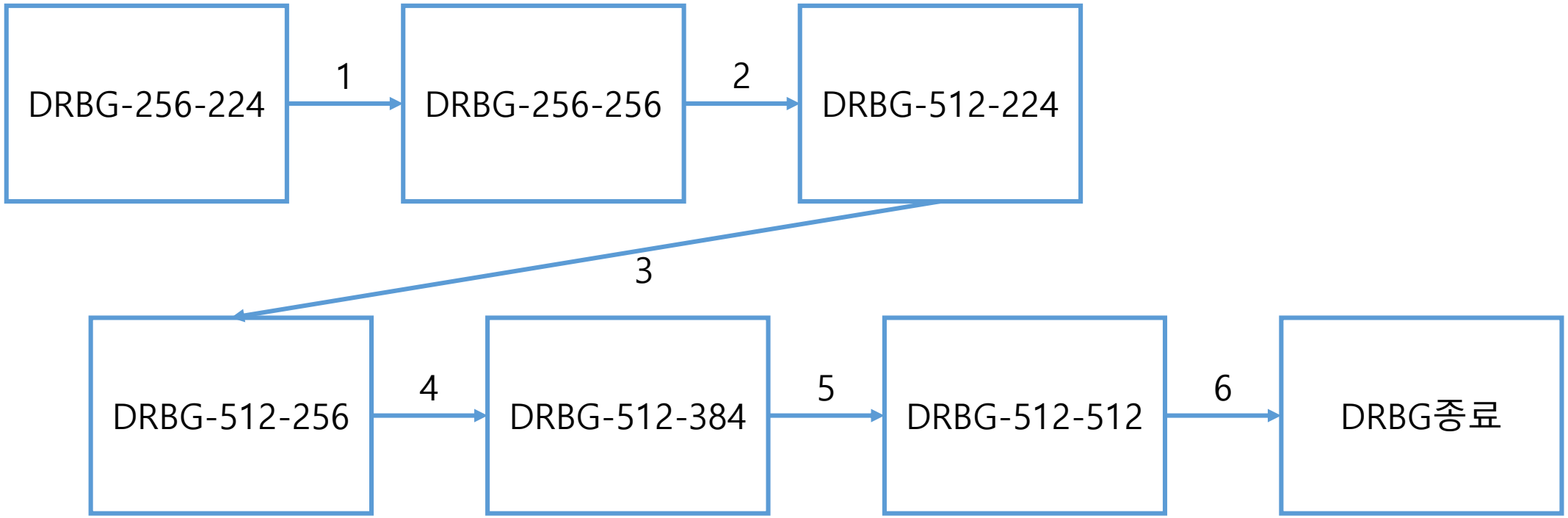
1.3 DRBG 내부 출력 생성 함수 구조

- 최대 2회까지 반복
  - 단, DRBG 출력에 비례
- w 값은 서로 독립



HSU HANSUNG UNIVERSITY

1.3 DRBG 전체 출력 구조



HSU HANSUNG UNIVERSITY

2. 실험 환경 구성

HSU
HANSUNG
UNIVERSITY

2.1 실험 환경 구성

운영체제	Windows 10 Pro
프로세서	Intel Core i7-8550U CPU 1.8GHz
컴파일러	MinGW
IDE	Eclipse Photon (4.8.0)
언어	C

2.1 실험 환경 구성

- LSH를 의사 난수로 사용하여 6개 규격 출력
- 모든 규격이 완료된 시점을 1회로 취급
- 테스트 벡터 60종을 1,000회에 반복
- 예측 내성 지원 설정

HSU
HANSUNG
UNIVERSITY

2.1 실험 환경 구성

- 데이터 병렬화
- 규격 별 출력을 병렬화
- 태스크 병렬화
- DRBG 내부 구조 병렬화
- 병렬화 기법을 적용한 모델과 병렬화 미적용 모델의 대조군을 비교

HSU HANSUNG UNIVERSITY

3. 성능 평가

HSU
HANSUNG
UNIVERSITY

3.1 데이터 병렬화 성능 평가

	평균 수행 시간(ms)	Clockcycle per Bytes(cpb)
대조군	73	491
병렬화	27	181

- 병렬화 적용 모델이 약 2.71배 향상된 성능
- 선행 규격 출력을 대기하는 시간이 제거됨

HSU HANSUNG UNIVERSITY

3.2 태스크 병렬화 성능 평가

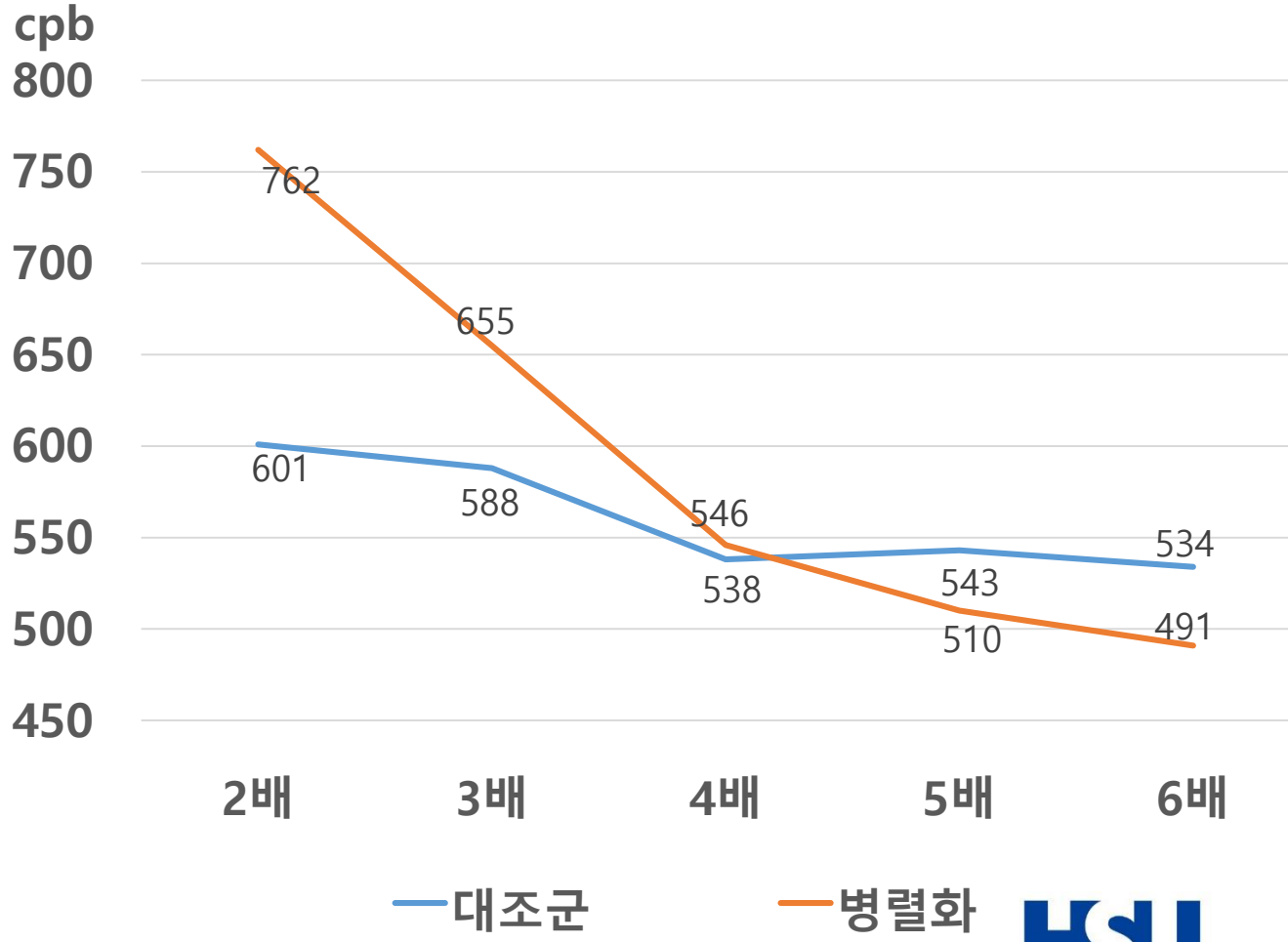
	평균 수행 시간(ms)	Clockcycle per Bytes(cpb)
대조군	73	491
병렬화	149	1001

- 병렬화 적용 모델이 약 2.04배 저하된 성능
- 병렬화 과정에서 발생하는 오버헤드로 판단
- 오버헤드를 경감시키기 위해 반복 횟수를 조절

HSU HANSUNG UNIVERSITY

3.2 태스크 병렬화 성능 평가

- 내부 출력 생성 함수는 출력 길이에 따라 반복 횟수가 증가
- 출력 길이 4배부터 근소한 차이
- 5배부터 병렬화 이득 발생



HSU HANSUNG UNIVERSITY

4. 결론

HANSUNG UNIVERSITY

4. 결론

- 데이터 병렬화 적용 시 성능 향상이 가능
  - 다수 규격 DRBG 출력 시 유용함
- 태스크 병렬화 적용 시 조건부 성능 향상이 가능
  - 단, 표준 규격과는 어긋나므로 실제 사용은 어려움

HSU HANSUNG UNIVERSITY

감사합니다

https://github.com/korLethean/DRBG_with_MP

HSU
HANSUNG
UNIVERSITY