HW8

1. **아래의 표를 채우시오(기한: 2월 20일 오후 6시)**
   1. 10,000의 연산에 대한 각 연산 별 결과값 확인 및 평균 연산 시간 측정

|  |  |  |
| --- | --- | --- |
| 연산 | 시간 | 비고 |
| 역원(Fermat Little Theorem 기반) | Debug: 1936443  Release: 331350 | 입력: TV\_opA.txt  정답: TV\_PFINV.txt |
| 역원(Binary Inversion 기반) | Debug: 285197  Release: 41156 |
| 아핀좌표계기반 ECADD, ECDBL,  LtR 스칼라 곱셈 | ECADD  Debug: 1423574  Release: 261564  ECDBL  Debug: 1243113  Release: 201281  LtR  Debug: 674278009  Release: 133838167 | 입력: TV\_Scalar.txt,  Base point(기저점)은 타원곡선강의자료 마지막 페이지에 있음  정답: TV\_SM.txt |
| Jacobian/Mixed좌표계기반 ECADD, ECDBL, LtR 스칼라 곱셈 | ECADD  Debug: 99097  Release: 18126  ECDDBL  Debug:49011  Release:8203  LtR  Debug: 23653530  Release: 5740204 |

1. **논문발표 준비(2월 21일 금요일)**

* 관련연구의 정리(Related Work, 기존 연구결과의 히스토리 정리)
* 논문의 핵심아이디어 파악 및 정리(어떤 방법을 통하여 어느정도 개선이 되었는지에 대한 내용 파악)
* (구현 재현을 위한)구현 환경에 대한 파악(장비, 컴파일러 등등)

|  |  |
| --- | --- |
| 담당 | 논문제목 |
| 안상우 | AES BitSlicing에 대한 소개+CHAM GPU 최적화 구현  : Fast AES Implementation A High-Throughput Bitsliced Approach |
| 송진교, 박보선, 민찬우 | - Fast AES implementation using ARMv8 ASIMD without cryptography extension(삼인방)  - All the AES you need on Cortex-M3 and M4  (송진교) |
| 최호진, 김영범, 이지원 | - FACE-LIGHT fast AES-CTR mode encryption for low-end microcontrollers(삼인방)  - PBKDF2 최적화 연구 결과 |