HW9

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 |
| Jacobian/Mixed좌표계기반 ECADD, ECDBL, LtR 스칼라 곱셈 | ECADD  Debug: 99097  Release: 18126  ECDDBL  Debug:49011  Release:8203  LtR  Debug: 23653530  Release: 5740204 | 입력: TV\_Scalar.txt,  Base point(기저점)은 타원곡선강의자료 마지막 페이지에 있음  정답: TV\_SM.txt |
| wNAF 기반의 variable point(unknown point) 스칼라 곱셈 | Debug: 25840046  Release: 5979516 | wNAF에서 w는 최대 6까지 범용적으로 설정할 수 있도록 구현(일반적으로 w=4로 많이 사용) |
| Comb 기반의 fixed point(known point) 스칼라 곱셈 | Debug: 14690944  Release: 3816838 | w=8로 하여 구현(총 256개의 포인트 저장) |

1. **연구진행**

* AVR 어셈블리 명령어 정리, ARM 어셈블리 명령어 정리
* 발표한 논문에 대한 구현
  + 본인들이 발표한 논문에 대한 구현 진행
  + 구현을 통해 확장 가능한 아이디어 도출
* 향후, AES 이외의 경량 블록암호 알고리즘 1종 선정  
  (<https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers> 참조)

|  |  |
| --- | --- |
| 담당 | 논문제목 |
| 안상우 | - AES BitSlicing에 대한 소개+CHAM GPU 최적화 구현  : Fast AES Implementation A High-Throughput Bitsliced Approach  - GPU 상에서 AES, CHAM에 대한 운영모드 최적 구현 |
| 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 : 향후 AVR 환경으로 확장, 재사용가능한 데이터의 테이블화 |

1. **github 가입 및 학생인증**

* AVR 어셈블리 명령어 정리, ARM 어셈블리 명령어 정리  
  (참조, <https://all-record.tistory.com/161>,  
  <https://m.blog.naver.com/PostView.nhn?blogId=rudtn082&logNo=221439717020&categoryNo=1&proxyReferer=https%3A%2F%2Fwww.google.co.kr%2F>)