공개키 암호의 구현

ECDSA 구현
YouTube: https://youtu.be/kijgVPJhdMA
Git: https://github.com/minpie/CryptoCraftLab-minpie_public

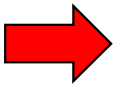
한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

발표 계획 목록

ECDSA C언어 구현

발표 계획: 24.11.09ver

- 대칭키 암호 단일블록 C언어 구현
  - 1. AES
  - 2. DES
- 64비트 이상 키 길이의 공개키 암호 C언어 구현
  - 3. GMP 라이브러리
  - 4. RSA 구현
  - 5. Rabin 구현
  - 6. Elgamal 구현
  - 7. ECDSA 구현 

- AES-운영모드 with 병렬컴퓨팅
  - 8. OpenMPI 라이브러리
  - 9. OpenMPI-AES
  - 10. CUDA C
  - 11. CUDA-AES

Q & A