//hyu.wiki/%EC%9E%84%EB%B2%A0%EB%94%94%EB%93%9C_%EB%B3%B4%EC%95%88%EC%8B%9C%EC%8A%A4%ED%85%9C_%EC%97%B0%EA%B5%AC%EC%8B%A4

임베디드 보안시스템 연구실

연구분야는 보안 SoC설계, PUF(Physical Unclonable Function), 모바일 금융결제, DPA 공격 방어 기법, GPGPU(General Purpose GPU) 병렬 처리로 나뉜다.

- 소속: 서울 공과대학 융합전자공학부
- 영문명: Embedded Security System Lab.
- 실장: 김동규 융합전자공학부 교수
- 홈페이지: http://esslab.hanyang.ac.kr/

□

목차

- 1 주요 연구
  - 1.1 보안 SoC설계
  - 1.2 PUF(Physical Unclonable Function)
  - 1.3 모바일 금융결제
  - 1.4 DPA 공격 방어 기법
  - 1.5 GPGPU(General Purpose GPU) 병렬 처리

주요 연구

보안 SoC설계

- 정보 누출 방지, 위변조 방지, 사용자 인증 등을 위한 다양한 암호 알고리즘과 프로토콜을 연구하며, 기존의 소프트웨어 보안방식의 취약점 극복과 효율성을 위해 전용 하드웨어 모듈을 구현하고 이를 검증한다.
- TPM(Trusted Platform Module)과 OTP(One Time Password)와 같은 보안 솔루션의 효율적인 구현 방법을 연구한다.

PUF(Physical Unclonable Function)

복제 불가능한 키의 저장 방법에 대한 연구를 수행한다.

모바일 금융결제

USIM을 이용한 사용자 휴대폰의 모바일 네트워크에 기반을 둔 결제 시스템을 연구한다.

DPA 공격 방어 기법

전력 분석에 의해 암호 알고리즘이 공격당하는 것을 막기 위한 기법을 연구한다.

GPGPU(General Purpose GPU) 병렬 처리

그래픽카드와 CUDA를 활용하여, 연산시간이 많이 걸리는 암호 알고리즘을 병렬로 처리하는 방안을 연구한다.