첨단암호기술연구실

(Advanced Cryptographic Technology Laboratory)

첨단암호기술연구실

- 지도교수: 하재철 (컴퓨터정보공학부, 제1공학관 512호)
- 연구실 위치: 제1공학관 511-4호

- 연구원 현황: 학석사연계 2명, 학부생 3명

- 연구 분야

- 암호 알고리즘 분석 및 설계
- 암호 알고리즘 고속화 및 최적화
- 양자 대응(Post-Quantum) 암호 분석 및 개발
- 부채널 공격(SCA) 및 방어
- 하드웨어 오류 주입 공격 및 대응
- 마이크로 아키텍처 공격 및 방어
- 네트워크 분석 및 악성 행위 탐지
- 인공 지능 시스템 보안
- 머신러닝 기반 보안 솔루션

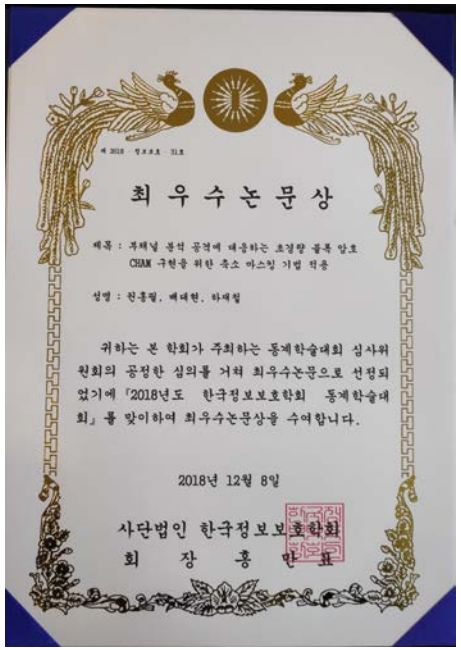
프로젝트

- 진행중
  - 양자 내성 암호에 대한 머신 러닝 기반 부채널 공격 및 대응 기술 개발 -1차년도(책임)
  - 상용 HW 암호 제품에 대한 공격 취약성 기술 연구 (책임)

- 종료 (최근 2년)
  - 전력 분석 공격에 대응하는 SM4 및 SM2 암호 알고리즘 설계(책임)
  - Crypto-Protector 검증용 암호 키 파형 데이터 셋 확보 및 분석(책임)
  - PQ 공개 키 암호의 오류 주입 대응 기술에 관한 연구(책임)
  - 경량 블록 암호 차분 전력분석 대응 기법 적용 방안 및 효율성 분석(책임)

연구 성과 (1/2) (최근 2년)

- 외부수상 4건



최 우 수 논 문 상

제목 : 부채널 분석 공격에 대응하는 초경량 블록 암호 CHAM 구현을 위한 축소 마스킹 기법 적용

성명 : 권홍찬, 배대현, 하재철

귀하는 본 학회가 주최하는 동계학술대회 심사위원회의 공정한 심의를 거쳐 최우수논문으로 선정되었기에 「2018년도 한국정보보호학회 동계학술대회」를 맞이하여 최우수논문상을 수여합니다.

2018년 12월 8일

사단법인 한국정보보호학회
회 장 홍 만 표

장 려 상

제목 : 중국 표준 블록 암호 알고리즘 SM4에 대한 전력 분석 공격 및 대응 기법

성명 : 배대현, 하재철(호서대학교), 남승현((주)파닉스)

위 사람은 2019년도 한국정보보호학회 춘계지부 학술논문발표회에서 우수논문상 수여자로 선정되어 이 상을 드립니다.

2019년 10월 18일

사단법인 한국정보보호학회
회 장 이 경 현

제 1635호

상 장

한국전자통신연구원 원장상
(고등/학부 부문)

호서대학교
배대현, 황윤배, 권홍찬

귀하의 비공개 암호 해독 결과가 「2019년도 부채널 분석 경진대회」 고등/학부 부문에서 최우수 결과으로 선정되었기에 이 상장을 드립니다.

2019년 10월 24일

한국전자통신연구원 원장 김 명 준

정보보호학회장상

제목 : 마이크로 컨트롤러 소비 전력 기반 명령어 수준 역어셈블러 구현

성명 : 배대현, 하재철 (호서대학교)

귀하는 본 학회가 주최하는 하계학술대회 심사위원회의 공정한 심의를 거쳐 최우수논문으로 선정되었기에 「2020년도 한국정보보호학회 하계학술대회」를 맞이하여 정보보호학회장상을 수여합니다.

2020년 7월 15일

사단법인 한국정보보호학회
회 장 정 수 환

연구 성과 (2/2) (최근 2년)

- KCI 논문 6편 (+2편 추가 개제 예정)


경량 암호 알고리즘 CHAM에 대한 오류 주입 공격

Fault Injection Attack on Lightweight Block Cipher CHAM


부채널 공격에 대응하는 경량 블록 암호 CHAM 구현을 위한 마스킹 기법 적용 및 분석

Application and Analysis of Masking Method to Implement Secure Lightweight Block Cipher CHAM Against Side-Channel Attack Attacks


Multi-Layer Perceptron 기법을 이용한 전력 분석 공격 구현 및 분석

Implementation and Analysis of Power Analysis Attack Using Multi-Layer Perceptron Method


블록 암호 SM4에 대한 부채널 공격 및 마스킹 기반 대응기법 분석

Side Channel Attack on Block Cipher SM4 and Analysis of Masking-Based Countermeasure


블록 암호 AES에 대한 CNN 기반의 전력 분석 공격

Power Analysis Attack of Block Cipher AES Based on Convolutional Neural Network


CNN을 이용한 소비 전력 파형 기반 명령어 수준 역어셈블러 구현

Implementation of Instruction-Level Disassembler Based on Power Consumption Traces Using CNN

- 국내/외 컨퍼런스 및 기타 논문 10편 이상
- 국내 특허 1건

More information

- http://islab.hoseo.ac.kr

Contact

- 하재철 교수님
  - jcha@hoseo.edu
  - 041-540-5991

- 연구실 대표 학생:
  - 배대현
  - noeyheadb@gmail.com
  - 010-3654-6726