고려대학교
KOREA UNIVERSITY

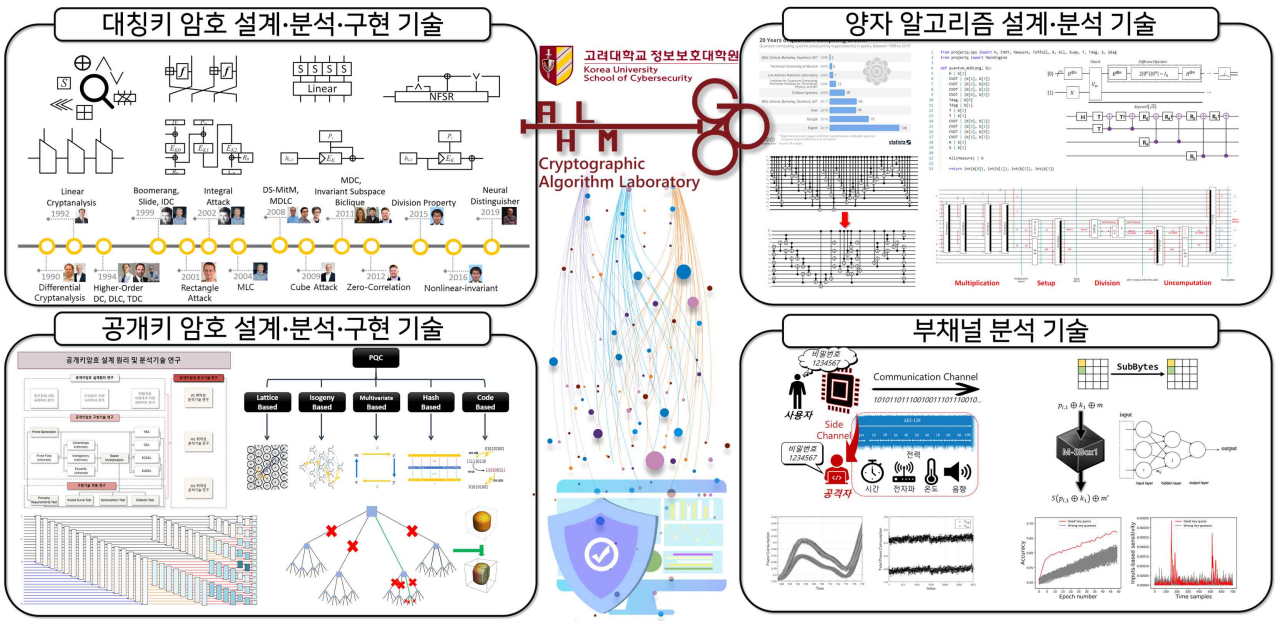
암호알고리즘 설계·분석·구현 기술

고려대학교 정보보호대학원 정보보호학과 암호알고리즘 연구실 (2021.12.21.)

홈페이지 : crypto.korea.ac.kr
연 락 처 : 02-3290-4756
메 일 : djpark@korea.ac.kr(박동준), cksgh419@korea.ac.kr(전찬호)

□ 소개

- 암호알고리즘 연구실은 1999년 정보보호대학원 설립의 기반이 된 연구실로 크게 대칭키·공개키 암호 알고리즘 연구, 양자 알고리즘 연구 및 부채널 분석 연구를 수행
- 각 연구 분야의 국가과제를 1건 이상 수행하고 있으며, SCI(E)급 저널 및 국제 유명 ASIACRYPT, FSE, CHES 등을 포함한 국제학회에 122건의 연구실적을 발표
- 암호암고리즘 연구실의 졸업생들은 대부분 교수 및 연구소, 대기업으로 진출하여 정보보호 및 암호 분야에 이바지함



□ 대칭키 암호 설계·분석·구현 기술

- 대칭키 암호 분야에서는 대칭키 암호알고리즘 설계, 구현 및 안전성 분석기술을 확보하고 있음
- 대칭키 암호알고리즘 설계에서는 대칭키 암호알고리즘을 이루는 컴포넌트(S-box, Linear layer)의 설계뿐만 아니라 상용 대칭키 암호알고리즘 또한 설계할 수 있는 기술을 확보하고 있음, 대표적으로 HIGHT, LEA, PIPO 등 다양한 대칭키 암호알고리즘을 설계함
- 2017년부터 국방과학연구소 과제인 "경량 구현 및 부채널 공격 대응 구현에 적합한 블록암호 설계 기술 연구" 과제를 통해, 블록암호의 경량성과 부채널 저항성에 초점을 맞춘 설계 기술 연구를 수행 중임
- 다양한 대칭키 암호알고리즘 공격 기법을 습득하여 실제 대칭키 암호알고리즘에 적용하며, 자동화된 안전성 분석 도구를 개발함
- 마찬가지로 2017년부터 국방과학연구소 과제인 "비선형 암호 논리 분석 및 병렬컴퓨팅을 활용한 암호 분석기술 연구" 과제를 통해, 블록암호의 안전성 분석과 병렬 CPU 및 GPGPU 고속화 기술 연구를 수행 중임

□ 공개키 암호 설계·분석·구현 기술

- RSA, DSA, ECC 등의 공개키 암호들은 금융계열, 통신계열 등에서 중요 핵심 기술로 활용되고 있음
- 기존의 공개키 암호들을 일반적인 PC 및 서버에서 활용할 수 있는 KLIB 라이브러리를 개발하여 KCMVP 검증필을 획득하고 상용화함
- 양자컴퓨터의 개발로 인하여 기존의 공개키 암호들의 안전하지 않게 될 미래를 대비하여, 양자컴퓨터의 공격에도 안전한 후양자암호(Post Qunaum Cryptography, PQC)의 개발이 필요성이 대두되고 있음
- 현재 후양자 공개키 암호 개발의 설계 및 구현 분야는 공개키 알고리즘의 특징인 연산속도와 저장 공간에 대한 단점을 완화하여 효율적인 공개키 알고리즘을 설계하고 구현하는 데에 목적이 있음
- 본 연구실에서는 다양한 환경에서 효율적으로 사용할 수 있는 후양자 암호 라이브러리의 개발 및 경량 디바이스에도 적용이 가능한 라이브러리 구현 연구를 진행중에 있음
- 또한 후양자 암호알고리즘의 안전성을 분석하는 알고리즘 및 도구의 최적화에 대해서도 함께 연구를 수행함

□ 양자 알고리즘 설계·분석 기술

- 양자 알고리즘 분야는 양자 컴퓨팅 환경에 대비하여 향상된 양자 알고리즘을 연구하고 각종 알고리즘의 양자 회로 설계 및 최적 구현을 진행함
- 양자 알고리즘을 활용해 현재 사용하고 있는 비밀키 암호 및 공개키 암호에 대한 향상된 분석 알고리즘 및 회로를 연구하고 계산 복잡도를 도출함
- 보다 정확한 계산 복잡도 분석을 위해 여러가지 유한체 연산과 NTT와 같은 여러 연산 기법에 대한 양자 회로를 설계함
- 연구 결과를 양자 프로그래밍 플랫폼 ProjectQ 등을 통해 시뮬레이션 회로로 구성하여 각 알고리즘에 대한 계산 복잡도를 실제로 측정함
- 시뮬레이션 결과를 바탕으로 향상된 알고리즘의 제시 및 최적 파라미터 선택 등에 대한 연구를 진행함
- 2019년부터 과학기술정보통신부 산하 정보통신기획평가원 과제인 '미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발' 과제를 통해, 현재 활발히 연구 중인 양자 내성 암호(PQC)에 대한 양자 컴퓨팅 환경에서의 양자 공격 복잡도를 분석하는 연구를 수행 중임

□ 부채널 분석 기술

- 부채널은 통신 당사자 간 합의된 채널이 아닌 모든 채널을 의미하며, 암호알고리즘이 수학적으로 안전하더라도 실제 구현물이 동작하는 환경 또는 구현 방식에 따라 부채널 정보에 의해 비밀정보가 드러날 수 있음
- 본 연구실은 상용보드(MCU, FPGA)에 분석 대상 알고리즘을 프로그램하거나 전력/전자파 부채널 정보를 수집하는데 필요한 장비, 높은 수준의 정밀도를 요구하는 오류주입(전압 글리치, 전자파/레이저 조사) 장비를 보유하고 있어 독립적인 부채널 분석 기술개발이 가능함
- 부채널 분석 연구 대상으로는 전통적인 비밀키 암호와 공개키 암호뿐만 아니라 화이트박스 암호, 후양자 암호, 양자 키분배, 딥러닝 알고리즘, 블록체인과 같은 최신의 이슈를 포함함
- 실제로 사용되고 있는 제품에 대한 분석 기술을 보유하고 있으며 그 예로는 IC 칩이 탑재된 선불 교통카드, 암호화폐의 송수신 및 키 저장 기능을 가진 하드웨어 지갑, 금융 어플리케이션이 실행되는 스마트폰 등이 있음