『PQC 구현 최적화 및 부채널 분석 기초 특강』

- Case-Study : CRYSTALS-KYBER, CRYSTALS-Dilithium

○ 일시 : 2022년 7월 18일 (월) 10:00 ~ 18:00

○ 장소 : 국민대학교 과학관 324호 (장소변경)

○ 주관 : 한국정보보호학회 부채널분석연구회, 국민대학교 차세대암호연구센터

○ 후원 : 고려대학교 IA&AI SecLab, 한성대학교 CryptoCraft Lab, 국민대학교 COALAB

○ 참석자 수(오프라인) : 100명 내외 (선착순)

○ 참가료 : 무료 (등록 마감 : 7월 8일 금요일 자정)

시간	발표주제	강사	내용
10:00 ~ 11:30	PQC 구현 최적화 기본 이론	권혁동 연구원 (한성대), 김영범 연구원 (국민대)	- NIST PQC 표준화 동향 소개 - NIST PQC 구현 플랫폼 소개 - 격자기반암호 기본 내용 소개 - 격자기반 PQC 2종 소개
11:30 ~ 13:00	점심		
13:00 ~ 14:30	PQC 구현 최적화 기본 내용 실습	권혁동 연구원 (한성대), 김영범 연구원 (국민대)	- 윈도우 환경 상에서 LWE 기반 차수 간소화 TOY 암호구현 - 윈도우 환경 상에서 다항식 곱셈 기본 알고리즘 구현
14:30 ~ 14:45	휴식		
14:45 ~ 16:15	부채널 분석 개론	한재승 연구원 (국민대)	- 부채널 분석이란? - 단순전력분석 ✓ AES, RSA 사례 - 1차전력분석 ✓ AES 실습
16:15 ~ 16:30	휴식		
16:30 ~ 18:00	PQC 부채널 분석 사례 소개	한재승 연구원 (국민대)	- PQC 단순전력분석 사례 ✓ Kyber, Dilithium 등 - PQC 1차전력분석 사례 ✓ 주요 연산 기반 분석