2023년 암호연구회 중간평가 워크샵

- 일 자 : 2023년 6월 1일 ~ 2일 (목,금)
- 주 최 : 한국정보보호학회
- 주 관 : 암호연구회
- 후 원 : 국민대학교 정보보안연구소
- 장 소 : 여수 소노캄

2023년 06월 01일 목요일			
시 간	멘 토	발 표 주 제	발표자
13:00~ 13:40	조지훈 (삼성SDS) 김기문(KISA)	美NIST-PQC 암호키 교환기법 및 성능비교 연구	서화정 (한성대학교)
13:40~ 14:20	손기욱 (서울과기대) 이일구 (성신여대)	암호 취약점 분석에 특화된 퍼징 기술 연구	권태경 (연세대학교)
14:20~ 15:00	윤영태 (NSR) 김창균 (NSR)	윈도우OS용 H/W암호모듈(TPM 2.0) 안전성 분석 연구	강병훈 (KAIST)
15:00~ 15:20	휴 식		
15:20~ 16:20	유일선 (국민대)	AIST/CPSEC의 소개와 국제 협력 방안	신성한 박사 (일본 국립 산업과학기술연구소)
16:20~ 16:40	휴 식		
16:40~ 17:20	김익균 (ETRI) 최형기 (성균관대)	가상화 난독화 적용 실행파일 분석연구	김도현 (부산가톨릭대학교)
17:20~ 18:00	권태경 (연세대) 이봉수 (NSR)	클라우드 환경에서의 개인정보 보호를 위한 딥러닝 고속화 연구	백윤흥 (서울대학교)

2023년 06월 02일 금요일			
시 간	멘 토	발 표 주 제	발표자
09:00~ 09:40	최두호 (고려대) 홍석희 (고려대)	DDR5 '로우해머'공격 암호학적 대응기법 연구	권건우 (홍익대학교)
09:40~ 10:20	진승헌 (ETRI) 최광희 (KISA)	非패스워드 방식의 안전성 분석 연구	최대선 (숭실대학교)
10:20~ 10:40	휴 식		
10:40~ 11:20	김은영 (NSR) 최병철 (ETRI)	리플레이기반 USB 입출력 시스템 보안기술 연구	송도경 (연세대학교)
11:20~ 12:00	김환국 (상명대) 강유성 (ETRI)	블록체인에 사용되는 다중 전자 서명 기법 분석 및 보안성 개선 연구	정익래 (고려대학교)