2021 KpqC SUMMER SCHOOL

양자내성암호의 기초

온라인 강연
QR코드

2021.6.23.(수) ~ 24.(목)

| 주최 | 양자내성암호연구단

대　　상 : 암호 기초 지식을 가진 누구나

운영방법 : 온라인 강연 - (https://youtube.com/channel/UCEgUkGK7fL7I2vrZgchaP9w)
- (https://url.kr/ofjvga) & QR 코드

양자내성암호에 사용되는 수학이론의 기초부터 암호설계 이론까지

프로그램

6월 23일 (수)

시간	교육	연사
10:00 ~ 12:00	격자 기반 암호	천정희 교수
13:30 ~ 15:30	다변수 기반 암호	심경아 팀장
16:00 ~ 18:00	코드 기반 암호	김종락 교수

6월 24일 (목)

시간	교육	연사
10:00 ~ 12:00	격자 기반 암호	천정희 교수
12:00 ~ 12:20	실시간 Q&A	
13:30 ~ 15:30	다변수 기반 암호	심경아 팀장
15:30 ~ 15:50	실시간 Q&A	
16:00 ~ 18:00	코드 기반 암호	심경아 팀장
18:00 ~ 18:20	실시간 Q&A	

연사 소개

천정희 교수

학력 및 경력

1997.02 - KAIST 이학박사 (정수론)
1997.02 ~ 2000.01 - ETRI 선임연구원
2000.01 ~ 2000.12 - Brown 대학 Visiting Scientist
2000.12 ~ 2003.02 - 한국정보통신대학교 조교수
2003.03 - 현재 서울대 수리과학부 교수
2016 - 현재 서울대 산업수학센터 센터장 (ERC)

강연 요약문

격자 암호는 격자기반의 NP-hard 난제에 기반하여 양자내성 (quantum-resilient)을 지니며, 이번 NIST PQC 표준화 공모전에서 가장 많은 스킴이 채택되었습니다. 본 강연에서는 격자이론의 기초부터 격자기반 난제, 그리고 이에 기반한 암호화, 전자서명 기술을 소개합니다. 특히, NIST competition의 3 라운드를 통과한 공개키암호/전자서명 스킴들을 소개하고 이의 활용에 대해서도 논의합니다.

심경아 팀장

학력 및 경력

이화여자대학교 수학과 이학박사
한국인터넷진흥원 암호기술팀 선임연구원
이화여자대학교 수학과 연구교수
(현)국가수리과학연구소 암호기술연구팀장

강연 요약문

1995년 Shor가 소인수분해문제와 이산대수문제를 다항식 시간 안에 풀어주는 양자알고리즘을 제안함에 따라, 현재 사용 중인 국제 표준 공개키 암호 RSA와 ECC는 양자컴퓨터가 개발되면 모두 깨진다는 것이 알려져 있습니다. 양자컴퓨터 이 후 시대의 정보보호를 위한 대안으로 양자컴퓨터에 안전한 공개키 암호의 연구가 활발히 진행되고 있습니다. 이 강연에서는 다변수 이차식 시스템의 해를 구하는 양자컴퓨터에 안전한 문제를 이용한 다변수 이차식 기반 공개키 암호의 설계와 안전성 분석을 소개하고자 합니다.

김종락 교수

학력 및 경력

서강대 수학과 교수
딥헬릭스 (주) CEO 및 설립자
루이빌 대학교 부교수
University of Illinois at Chicago 박사
Kirkman medal 수여
Designs, Codes and Cryptography 저널 편집위원
<Concise Encyclopedia of Coding Theory> 공동 편집자
<보드게임하는 수학자> 저자

강연 요약문

이번 강연에서는 부호 기반 공개키 암호를 소개합니다. 부호는 Coding Theory에서 등장하는 오류 정정 부호를 말합니다. 부호론은 Claude Shannon이 1948년에 시작한 정보이론의 핵심이론입니다. RSA암호와 비슷한 시기에 McEliece가 최초의 부호 기반 암호를 만들었는데 이것이 오늘날까지 유지되고 있습니다. NIST PQC 표준화 공모전에 등장하는 부호 기반 암호는 대부분 McEliece 암호를 그대로 사용하거나 변형된 형태입니다. 부호론의 기초부터 최신 이론까지 학부생 수준으로 강연을 진행할 예정입니다.