2022 KpqC Summer School

- **양자내성암호의 기초 II**
  - 양자내성암호에 사용되는 수학이론의 기초부터 암호설계 이론까지
  - '21년에 개최된 양자내성암호의 기초 I은 www.kpqc.or.kr 참조
- **2022. 6. 8. (수) 10:00 ~ 17:30**
- **주관 :** 양자내성암호연구단
- **대상 :** 암호기초지식을 가진 누구나
- **운영방법 :** 온라인 강연 youtube.com/KpqC연구단
  ※ 등록 및 참가비 없음

프로그램

시간	교육	강사	진행
10:00 - 12:00	영지식 증명과 암호	서재홍 교수 (한양대)	이광수 교수 (세종대)
13:00 - 15:00	아이소제니 기반 암호	윤기순 박사 (NSHC)	서승현 교수 (한양대)
15:30 - 17:30	해시 기반 암호	이주영 교수 (KAIST)	서화정 교수 (한성대)

강사소개

서재홍 교수

학력 및 경력

- 서울대학교 수리과학부 이학박사
- 일본 국가정보통신기술연구소
- 명지대학교 수학과 조교수, 부교수
- (현)한양대학교 수학과 부교수

강연 요약문

영지식 증명은 인증이나 전자서명과 같은 기초 암호 설계 논리와도 밀접한 연관이 있으며 프라이버시 향상을 위한 중요한 암호학적 설계도구로서 다양한 분야에서 널리 활용이 되고 있습니다. 본 강연에서는 영지식 증명의 기본개념, 인증 및 전자서명과의 연관성, 그리고 영지식 증명을 이용한 양자내성 전자서명 설계방법론에 대해 소개하고자 합니다.

윤기순 박사

학력 및 경력

- Université de Caen Normandie 이학박사(산술기하, 암호학)
- KSIGN, SoftForum에서 암호/인증 시스템 개발
- 국민대, 고려대 등에서 암호학강의
- 차세대 보안리더 양성 프로그램 (BoB) 멘토
- (현)NSHC 암호기술연구소 소장

강연 요약문

본 강연에서는 아이소제니-기반 양자내성 암호를 이해하기 위한 아이소제니 기초 이론을 소개합니다. 정층이 군(group)과 체(field)의 기본적 사항들에 대해 알고 있다고 가정하고 기하학적 개념들을 통해 타원곡선의 연산과 아이소제니에 대해 설명합니다. 또한 암호학적 응용에서 아이소제니를 설계로 계산하기 위한 벨류의 공식(Velu's formulae)을 소개합니다.

이주영 교수

학력 및 경력

- University of Waterloo 이학박사(암호론)
- 국가보안기술연구소 선임연구원
- 세종대학교 조교수/부교수
- (현)KAIST 전산학부 (정보보호대학원) 부교수
- (현)KAIST 정보보호대학원 책임교수
- (현)대한수학회 암호학 분과위원장

강연 요약문

해시 함수 기반 전자서명은 해시 함수만을 사용하여 설계되므로, 대수적 난제에 기반하지 않는 최소화된 안전성 가정으로 증명가능한 안전성을 제공합니다. 이러한 장점으로 인해, 해시 함수 기반 전자 서명 SPHINCS+는 NIST PQC 최종라운드 후보에 포함되었습니다. 본 강연에서는 해시 함수의 일반적인 성질과 설계 방식에 대해 살펴보고, 다양한 해시 함수 기반 전자 서명에 대하여 알아봅니다.