


# KpqC WINTER CAMP

# 2025

'26. 2. 24.(화) ~ 26.(목)

- 장 소** 서강대학교 정하상관 102호
- 내 용** KpqC 알고리즘 이해 및 구현에 필요한 기술
- 주 관**  양자내성암호연구단
- 대 상** 양자내성암호에 관심있는 누구나 (알기 쉽고 평이하게 진행)
- 참가신청** <https://forms.gle/YTCiHSpGSfnxuWEt5> (참가비 무료)
- 신청기한** '26. 2. 8.(일)
- 문 의** kpqcrypto@gmail.com



	시간	내용	발표자
2.24. (화)	13:30 - 14:30	KEM 의 이론적 안전성 이해	이주희 교수(성신여대)
	14:40 - 15:40	전자서명의 이론적 안전성 이해	이형태 교수(중앙대)
	15:50 - 16:50	키공유 프로토콜과 PQ/T 하이브리드 이해	손용하 교수(성신여대)
2.25. (수)	13:30 - 14:20	NTRU+: 알고리즘, 참조코드 및 활용방안 소개	김종현 박사(고려대)
	14:30 - 15:20	SMAUG-T: 알고리즘, 참조코드 및 활용방안 소개	김태경 박사(크립토랩)
	15:30 - 16:20	AIMer: 알고리즘, 참조코드 및 활용방안 소개	김성광 박사(삼성 SDS)
	16:30 - 17:20	HAETAE: 알고리즘, 참조코드 및 활용방안 소개	김태경 박사(크립토랩)
2.26. (목)	13:30 - 14:30	KEM 알고리즘 최적 구현 기술	서화정 교수(한성대)
	14:40 - 15:40	전자서명 알고리즘 최적 구현 기술	
	15:50 - 16:50	PQC 알고리즘 HW 구현 기술	이봉수 박사(국보연)