KpqC 연구단 7차 워크숍

날 짜 2023. 11. 13.(월) ~ 11. 14.(화)
장 소 연세대학교 동문회관 3층 그랜드볼룸
내 용 KpqC 공모전 1라운드 알고리즘 분석 결과 및 개선 내용 발표
대 상 양자내성암호에 관심있는 누구나
참가신청 https://forms.gle/qEzSVYThjvdwkjME8 (참가비 무료)
신청기한 11. 3.(금)
주 관 양자내성암호연구단

시간		발표제목	발표자
11. 13. (월)	13:30 ~ 14:00	How to meet low entropy LWE keys	이창민 교수(KIAS)
	14:00 ~ 14:30	KpqC 공모전에 제안된 Fiat-Shamir 기반 래티스 서명 기법의 안전성 증명 분석	박종환 교수(상명대)
	14:30 ~ 15:00	KpqC 공모전 1라운드 격자기반 알고리즘 안전성 분석	이주희 교수(성신여대)
	15:00 ~ 15:30	**휴 식**	
	15:30 ~ 15:40	**NTRU+ 개선사항**	**김종현 연구원(고려대)**
	15:40 ~ 15:50	**HAETAE update to v1.1**	**최형민 연구원(서울대)**
	15:50 ~ 16:00	**SMAUG update to v1.1**	**성효은 연구원(크립토랩)**
	16:00 ~ 16:10	**TIGER 개선사항**	**박승환 사무관(방첩사)**
	16:10 ~ 16:20	**Recent Updates on SOLMAE**	**김광조 원장(국사원)**
	16:20 ~ 16:30	**IPCC7 update**	**류지은 연구원(국민대)**
	16:30 ~ 17:00	KpqC 공모전 관련 안내	정경철 실장(국보연)
11. 14 (화)	13:30 ~ 14:00	KpqC 코드기반 알고리즘 안전성 분석	김종락 교수(서강대)
	14:00 ~ 14:30	KpqC 공모전 알고리즘 기본 구현에 대한 성능 비교 분석	서화정 교수(한성대)
	14:30 ~ 15:00	KpqC 암호의 경량 프로세서 구현특징 분석	김호원 교수(부산대)
	15:00 ~ 15:30	휴 식	
	15:30 ~ 16:00	KpqC 공모전 알고리즘 부채널 안전성 분석	김희석 교수(고려대)
	16:00 ~ 16:10	**Improvements of MQ-Sign and NCC-Sign**	**심경아 본부장(NIMS)**
	16:10 ~ 16:20	**Layered ROLLO 공격 시나리오 및 개선점 분석**	**김찬기 교수(전북대)**
	16:20 ~ 16:30	**AIM에 대한 분석 및 대응**	**하진철 연구원(KAIST)**
	16:30 ~ 17:10	**KpqC 공모전 알고리즘 종합 분석**	T.Lange 교수(아인트호벤대)