I N V I T A T I O N

2022

Quantum Risk 대응을 위한 Quantum Security

양자보안연구회 워크숍

2022년 10월18일(화) 12:00-18:00

서울 엘타워 8층 엘하우스 온라인/오프라인 진행

공동 운영위원장 이원혁(KISTI)

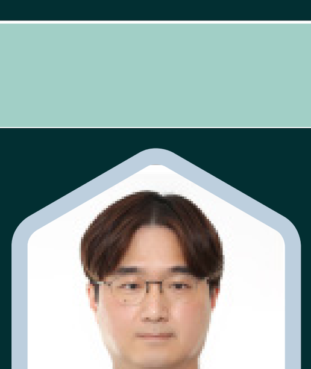
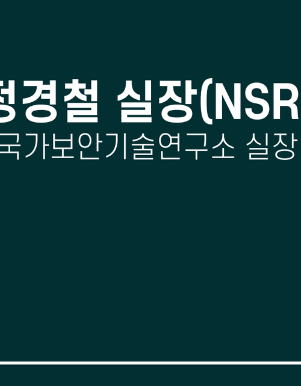
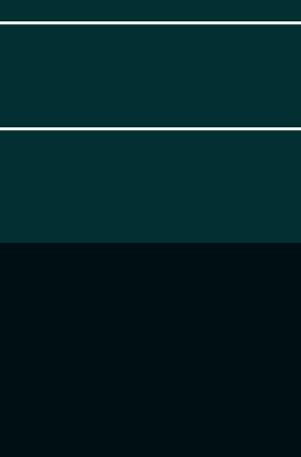
국가적으로 투자가 가속화되고 있는 양자관련 기술들은 다양한 분야에서 원천 기술에 대한 연구 및 활용성에 대한 고민이 진행되고 있습니다. 양자컴퓨터의 개발연구는 물론, 양자암호통신, 양자통신 기술들에 대한 연구 스펙트럼이 점차 확대되고 있는 상황에서, 양자보안기술 연구 활동도 탄력을 받고 있습니다. 본 워크숍에서는 현재 우리나라에서 수행되고 있는 양자보안 기술의 현황을 소개하고, 양자보안 연구와 활용강화를 위한 산업계, 학계, 연구계의 교류 협력의 기회가 되기를 희망합니다.

공동 운영위원장 최두호(고려대)

이번 워크숍은 양자기술 발전으로 인한 양자리스크 대응을 위한 양자보안 기술 현황을 살펴보고 토의하는 시간으로 마련하였습니다. 산·학·연에서 양자기술 분야를 연구하시는 전문가들을 모시고 최신 기술 현황과 적용사례를 살펴보고자 합니다. 양자보안을 포함하여 양자리스크를 대응하는 양자기술들에 대해서 경청하고 토론하는 좋은 자리가 되시길 기대합니다.

• 프/로/그/램 •

- **공동프로그램위원장**: 김익균 본부장(ETRI)/석우진 책임(KISTI)
- **프로그램 위원:**
  허준(고려대), 김효실(FQCF), 이성재(KISA), 강유성(ETRI), 권대성(NSR), 손일권(KISTI), 홍석희(고려대), 김호원(부산대), 이만희(한남대), 한동국(국민대), 김기문(KISA), 조기현(KISTI), 서화정(한성대), 이석준(가천대), 김용환(KISTI)

10월18일(화)	내 용	발 표 자
11:00 ~ 12:00	양자보안연구회-한국암호포럼 양자암호전문가 간담회 (비공개)	
12:00 ~ 13:00	등록 (8층 엘하우스)	
	세션1: 초청/기조강연 및 개회식 (사회 석우진 책임)	
13:00 ~ 13:30	**(초청강연) 양자컴퓨터의 기술수준 동향 및 향후 전망** 양자컴퓨터는 디지털 컴퓨터와는 다른 양자알고리듬을 구현할 수 있어 암호분야에서 큰 관심을 받고 있다. 양자컴퓨터 기술은 지난 20여년간 눈부시게 발전해왔지만 한편으로 실용적인 대규모 양자컴퓨터의 등장은 아직 시간이 더 필요한 것으로 생각된다. 본 발표에서는 양자컴퓨터의 최신 기술수준 동향과 발전 전망을 살펴보고, 적절한 전략적 대응을 고민해보기로 한다.	 정연욱 교수(성균관대) 성균관대학교 나노공학과 교수
13:30 ~ 13:40	개회사 및 환영사 (한국정보보호학회 회장 이옥연 교수)	
13:40 ~ 13:50	축사 (과기정통부)	
13:50 ~ 14:20	**(기조강연) 양자 시대를 향한 산업계 대응 전략** 산업계에서는 이미 아날로그 기술의 디지털 전환이 가속화되고 있는 반면, 양자기술은 이제야 Science 영역에서 Industry로의 전환을 시작하고 있다. 미-중 기술패권 경쟁, 글로벌 공급망 붕괴, 기술자원 부족이라는 Trilemma에 직면한 국내 양자산업계가 지향해야 할 양자시대로의 진화 논리와 그 대응 방안을 소개한다.	 KT 김이한 원장 KT 융합기술원 원장 미래양자융합포럼 공동의장
14:20 ~ 14:30	휴식	
	세션2: 양자리스크 대응 현황 (사회 최두호 교수)	
14:30 ~ 15:00	**양자 리스크 대응을 위한 양자암호통신망 구축 개발과 활용 연구** 양자컴퓨터의 대두에 따른 보안대응 방안이 여러 측면으로 고려되고, 연구가 진행되고 있다. 본 발표에서는 양자암호통신을 위한 양자키분배기술과 표준화 기반의 양자키관리 시스템의 개발 진행 사항을 소개하고, 출연연구소나 대학에서 진행하고 있는 양자통신의 실망 테스트 지원 등의 사례를 바탕으로 활용연구 활동을 소개한다.	 이원혁 팀장(KISTI) 한국과학기술정보연구원 양자&차세대연구망 팀장
15:00 ~ 15:30	**NIST PQC 3라운드 표준 후보였던 Rainbow에 대한 양자안전성 분석** 최근 발표된 Rank기반 키복구 공격기법들은 반복적인 커널찾기 속도를 높여 NIST PQC 3라운드 후보알고리즘이었던 Rainbow의 보안수준을 낮췄다. 이러한 반복적인 작업을 수행하는 부분에 양자 알고리즘을 적용하면 Rank기반 공격은 더 위협적인 공격이 될 수 있으며, 본 발표에서는 Rainbow의 키복원 공격을 위해 양자 알고리즘을 최초로 접목한 Q-rMinRank 공격을 소개한다. 새로운 공격방법을 통해 Rainbow의 모든 보안 파라미터 집합이 NIST에서 설정한 최소 보안 요구 사항을 충족하지 않음을 보인다.	 서승현 교수(한양대) 한양대학교(ERICA) 전자공학부 교수
15:30 ~ 16:00	**양자시뮬레이터 활용 사례: <Q|Crypton> 활용 양자 AES 구현** 대칭키 암호의 양자 보안강도를 검증하기 위해서는 검증 대상 암호를 양자회로로 구현할 필요가 있다. 구현에 사용된 큐비트수나 게이트 수 등은 암호의 양자 보안강도를 검증하기 위한 주요 양자자원량이다. 본 발표에서는 ETRI 양자안전성 검증 플랫폼인 <Q|Crypton>를 활용하여 대칭키 암호인 AES를 양자회로로 구현하고 양자 자원량을 분석하는 방법을 소개한다.	 이유석 박사(ETRI) 한국전자통신연구원 선임연구원
16:00 ~ 16:30	**양자내성암호 국가공모전 소개** 양자 암호분석 알고리즘과 양자 컴퓨터 개발 기술의 발전에 따른 암호 분야의 대응 필요성이 지속해서 제기되고 있다. 양자 컴퓨터 공격에도 안전한 양자내성암호 개발을 위해 국제적으로 어떠한 활동들이 전개되고 있는지 간략하게 살펴보고, 국내에서 진행되고 있는 '양자내성암호 국가공모전'에 대해서 소개한다.	정경철 실장(NSR) 국가보안기술연구소 실장
16:30 ~ 16:40	휴식	
	세션3: 양자기술 국내 현황 (사회 강유성 실장)	
16:40 ~ 17:10	**고에너지 입자물리학에서 양자정보기술의 활용** 입자물리학에서는 다양한 실험들에서 오는 데이터 분석을 통해 새로운 물리학의 흔적을 찾는다. 이러한 새로운 물리법칙의 탐구에 있어서 (1)양자컴퓨터 및 양자어닐러의 활용, 그리고 (2)양자상태 얽힘에 대한 실험적 측정에 대해 알아본다.	 박명훈 교수(서울과기대) 서울과학기술대학교 부교수
17:10 ~ 17:40	**양자오류정정 기법의 개념 및 응용** 양자컴퓨터를 구형하기 위해서는 물리적 잡음 및 간섭 등에 의해서 발행하는 양자 오류를 검출 및 정정하여 사용자가 오류의 걱정 없이 양자컴퓨터를 활용할 수 있는 환경을 제공해야 합니다. 본 강의에서는 양자오류정정 기법의 원리 및 개념을 설명하고 현재 응용되고 있는 기술을 소개합니다.	 허준 교수(고려대) 고려대학교 전기전자공학부 교수
17:40 ~ 18:10	**베타선을 이용한 양자난수생성기술** 인류가 암호화를 고안하고 난수를 사용하기 시작한 1882년부터 지금까지 보안분야에서 가장 필요로 했던 기술이 '순수난수를 고속으로 생성할 수 있는 장치' 이다. 하지만 현실세계에서는 생각보다 순수난수를 얻을 방법이 그리 많지 않았으며 더구나 컴퓨터 속도의 발전, 통신 단말의 소형화와 보조를 맞출 수 있는 '경량화된 고속 순수난수발생 장치'는 매우 어려운 기술중 하나로 여겨지고 있다. 이에 최근 몇년간 여러 연구 그룹에서 이와 관련된 기술들을 발표하고 있으며, 이 가운데 베타선을 이용한 양자난수생성기술을 본 발표에서 소개하고자 한다. 순수난수를 얻기에 가장 완벽한 랜덤소스라고 알려진 '동위원소의 자연붕괴 양자현상'중 베타선을 이용하는 '고속/경량 양자난수발생기를 구현하는 기술'을 주내용으로 하고 있다.	 박경환 박사(ETRI) 한국전자통신연구원 실장
18:10 ~ 18:20	마무리	

• 등/록/안/내 •

등록비

학생 10만원 | 일반 20만원

사전 등록안내

- 사전등록은 **2022년 10월 17일 월요일 오후 4시까지**입니다.
- 코로나바이러스 상황으로 인해 온라인/오프라인 병행으로 진행됩니다.
- 사전등록방법
  * 학회홈페이지 접속 ▶ 학술행사 ▶ 국내학술대회 ▶ 사전등록바로가기 클릭
- 사전등록 송금처
  * 예금주 : 한국정보보호학회
  * 계좌번호 : 사)한국정보보호학회 / (국민은행) 754201-04-135666
  ※ 양자보안연구회 전용계좌입니다.
- 사전등록시 위의 구좌로 송금하시고, 입금자가 대리인일 경우 통보 바랍니다.
- 신용카드 결제시 세금계산서 발급이 불가합니다 (부가가치세법 시행령 제 57조)

등록 문의처

- 전화: 02-564-9333~4(내선5)
- 메일: kiisc@kiisc.or.kr
- 프로그램그램 관련 문의: 042-869-1633 김기욱 박사(KISTI)

주관 한국정보보호학회 Korea Institute of Information Security & Cryptology 양자보안연구회

후원 미래양자융합포럼 Future Quantum Convergence Forum / KISTI 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr / ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute / KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY