





## 배포 즉시 보도 가능합니다.

대전(본원): 대외협력실 이종성 042-869-0976 / 이해준 0676 / 손영주 0997

문의: 과학기술연구망센터 이원혁 책임연구원(042-869-0648)

배포번호: 2021-30

배포일자 : 2021.09.29.(수)

매수 : 보도자료 4매

(첨부자료 포함)

배포처 : 대외협력실

## KISTI, 한국정보보호학회와 양자보안연구회 워크숍 개최

- 양자보안기술 글로벌 협력 및 산업 활성화 전략 논의 -

한국과학기술정보연구원(원장 김재수, 이하 KISTI)과 한국정보보호학 회는 양자보안기술 글로벌 협력과 산업 활성화 전략을 위하여 9월 29일 KISTI 대전본원 키움관에서 2021년 양자보안연구회 워크숍을 개최한다.

최근 양자컴퓨터 개발연구가 진행되면서 현존하는 암호 프로토콜들의 안 전성문제를 보완하고 발전시키기 위해. 공개키 암호 알고리즘을 대체할 수 있는 방안에 대한 관심이 높아지고 있다. 양자 보안기술이 더욱 중요해짐 에 따라 KISTI와 한국정보보호학회 등 산학연 기관들은 지난 1월 15일 두 분야 간 학문적인 발전을 도모하고자 양자보안연구회를 설립하였다. 양자 보안연구회는 과학기술정보통신부의 미래양자융합포럼 보안국제협력분과 역할도 동시에 수행 중이다.

이번 워크숍은 해외 양자보안 기술발전에 대비한 국내 산·학·연들의 대응 전략에 대한 행사로, 4개 세션으로 나눠 다양한 분야별 발표를 통해 양자키 분배(QKD, Quantum Key Distribution)\*, 양자내성암호(PQC, Post-Quantum Cryptography)\*\*에 대한 연구 현황과 기술 표준 동향을 알아볼 수 있다.

- \* 양자키분배(QKD): 양자역학적 성질을 이용하여 도청으로부터 안전하게 대칭키를 나누 어가질 수 있는 키 분배 기술
- \*\* 양자내성암호(POC): 양자컴퓨터로도 풀기 어려운 복잡한 수학 알고리즘을 사용한 암호



특히 그동안 국내 위주의 협력을 벗어나 미국, 일본, 유럽의 양자보안 기술 발표와 국내 산업 활성화를 위한 글로벌 협력 및 보안 기술 경쟁력 확보를 위한 국가 정책 방향이 논의된다.

KISTI 김재수 원장은 "양자보안 기술은 QKD와 PQC 중심으로 빠르게 발전하고 있으며, 공공기관 및 출연연의 데이터 보호를 위하여 KISTI가 중점사업으로 추진하고 있다. 미국 등과의 선진기술 협력이 필요한 시점이 되었고 이번 워크숍이 좋은 교류의 장이 될 것으로 기대한다"고 말했으며.

한국정보보호학회 회장인 충남대학교 컴퓨터공학과 류재철 교수는 "양자보안연구회는 산·학·연에서 수행되는 양자기술을 활용한 보안연구에 대해서 정보를 교류하고 기술을 협력할 수 있는 학문 교류의 장(Academic Playground) 역할을 수행하고자 한다. 이번 양자보안연구회 하반기 워크숍을 통하여 국내외 QKD, PQC 기술의 동향을 파악하는데 도움이 되길 기대한다"고 말했다.



첨부

## 2021년 양자보안연구회 워크숍 안내 배너 및 포스터













