정부혁신 보다 나은 정부	보 도 자 료	한국과학기술정보연구원 Korea Institute of Science and Technology Information
배포 즉시 보도 가능합니다.		
대전(본원): 대외협력실 이종성 042-869-0976 / 이해준 0676 / 손영주 0997 문의: 과학기술연구망센터 석우진 센터장(042-869-0596)		
배포번호 : 2021-03 배포일자 : 2021.02.01.(월)	매수 : 보도자료 2매 (첨부자료 별첨)	배포처 : 대외협력실

KISTI, 양자보안기술연구 추진

- 한국정보보호학회에 양자암호연구회를 설립하여 간사 역할 -

- 양자 및 보안 기술에 대한 기술 표준 및 방향성 제시가 목적 -

한국과학기술정보연구원(원장직무대행 조금원, 이하 KISTI)은 한국정보보호학회 내에 '양자보안 연구회'를 설립하여 간사 역할을 맡아, 차세대 컴퓨팅 및 보안 기술로 각광받는 양자·보안 기술 연구에 본격적으로 나선다.

양자컴퓨터의 출현으로 암호 알고리즘의 안전성 문제가 대두되어 현재의 공개키 방식 암호 알고리즘을 대체할 수 있는 방안이 필요해지고 있다. 이에 양자·보안기술에 대한 중요도가 높아짐에 따라 한국정보보호학회에서는 지난 1월 15일 두 분야 간 학문적인 발전을 도모하고자 양자보안 연구회를 설립하였다.

전자금융거래에서 인증과 전자서명에 사용되는 공개키 방식의 암호 알고리즘은 소인수분해와 이산대수 문제 등에 기반을 두어 개인키와 공개키를 만들어 사용한다. 공개키 알고리즘의 안전성은 이러한 수학적 문제와 직결되며, 문제의 해를 구하기 위해서는 전 세계 모든 슈퍼컴퓨터를 사용하더라도

수십 년 이상 소요된다. 하지만 양자컴퓨터의 초고속 연산처리 성능으로 사용자들이 비밀로 사용하고 있는 개인키를 쉽게 찾을 수 있는 상황이 발생하게 된다.

정보보호학회에 따르면 해당 연구회는 산업계, 학계, 연구소 등 양자·보안기술 분야의 전문가들이 참여하여 다가오는 양자컴퓨터 시대를 대비하기 위해 △양자키분배(QKD, Quantum Key Distribution) △양자내성암호(PQC, Post-Quantum Cryptography) 등을 연구하고, 기술 표준과 방향성을 제시할 수 있는 토론의 장을 만드는 데 목적을 두고 있다. 더불어 연구회 참여자들 간 관련 기술을 공유하고, 양자·보안 기술 세미나와 교육을 개최하여 산학연 정보교류에 기여할 계획이다.

한국정보보호학회장 류재철 충남대학교 컴퓨터융합학부 교수는 "양자·보안기술은 한국정보호호학회 회원들이 많은 관심을 갖고 있는 미래 기술로 산·학·연 전문가들의 활발한 활동을 기대하며, 학회에서도 양자암호 연구회의 발전을 위한 끊임없는 지원을 하겠다"고 양자보안 연구회 설립에 대한 계획을 밝혔다.

한국전자통신연구원(ETRI) 김익균 정보보호연구본부장은 "미래 양자컴퓨터 시대에 예견되는 기존 암호체계 무력화 위협에 적극적으로 대비하기 위해 출범한 본 양자보안 연구회가 양자·보안기술의 연구 개발에 중심적인 역할을 할 것으로 기대된다"라고 축하를 전했다.

이에 양자보안 연구회의 간사를 맡은 KISTI 석우진 과학기술연구망센터장은 "본 연구회 활동을 통해 양자보안 기술이 KISTI의 국가 과학기술연구망에 접목될 수 있도록 참여자들의 협력과 연구 성과 창출에 지속해서 노력하겠다"라는 포부를 내비쳤다.