

'차세대 암호 알고리즘 양자내성암호' 특허, 조선대 11건 보유

류형근 기자 입력 2023. 3. 14. 11:26

기사내용 요약

김영식 정보통신공학부 교수 국내외 특허 20여건



[광주=뉴시스] 조선대학교 *재판매 및 DB 금지

[광주=뉴시스] 류형근 기자 = 조선대학교가 양자내성암호(포스트양자암호) 기술과 관련한 특허를 11건 보유하고 있는 것으로 나타났다.

14일 조선대가 특허청이 지난 1월 발표한 자료를 토대로 분석한 결과에 따르면 차세대 암호 기술 시장을 주도할 수 있는 양자내성암호와 관련된 특허를 11건을 보유하고 있는 것으로 확인됐다. 또 김영식 정보통신공학부 교수가 양자내성암호와 관련된 특허 20여건을 보유하고 있다.

조선대 보유 양자내성암호 관련 특허는 크립토탭(25건), 삼성(18건), 서울대학교(12건)에 이어 4위이다. 세계에서는 23위인 것으로 확인되고 있다.

조선대가 보유하고 있는 양자내성암호와 관련된 특허는 '거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치 및 동작 방법'을 비롯해 '더티 페이퍼 코딩을 통한 전자 서명이 가능한 데

이더 전송 장치 동작 방법' 등이다.

또 '데이터 보안이 강화된 전자 서명 장치 및 방법' '패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치 및 방법' 't+a개의 오류 코드가 삽입된 부호 기반의 암호화 데이터의 복호화가 가능한 전자 장치 및 동작 방법'이다.

김영식 교수는 지난 2011년부터 올해까지 양자내성암호에 대한 연구를 지속해서 진행해 국내외 특허 20여건을 보유하고 있으며, 양자내성을 갖는 동형암호에 대한 40여 건의 국내외 특허를 등록 및 출원했다.

조선대 관계자는 "양자내성암호는 양자컴퓨터에서도 효율적인 계산이 어려운 새로운 형태의 수학 난제에 기반을 둔 암호 알고리즘이다"며 "최근에는 양자내성암호는 양자 컴퓨터에 대한 안전성을 제공하고 디지털 시스템에서 구현이 가능해 차세대 암호기술로 떠오르고 있다"고 밝혔다.

이어 "조선대는 양자내암호 특허를 다수 보유하고 있어 관련 산업의 연구를 주도할 것으로 기대된다"며 "앞으로 양자내성암호 기술 내재화와 안정적인 체계 전환을 위한 연구에 더욱 집중할 방침이다"고 밝혔다.

✉공감언론 뉴시스 hgryu77@newsis.com

© 공감언론 뉴시스통신사. 무단전재-재배포 금지