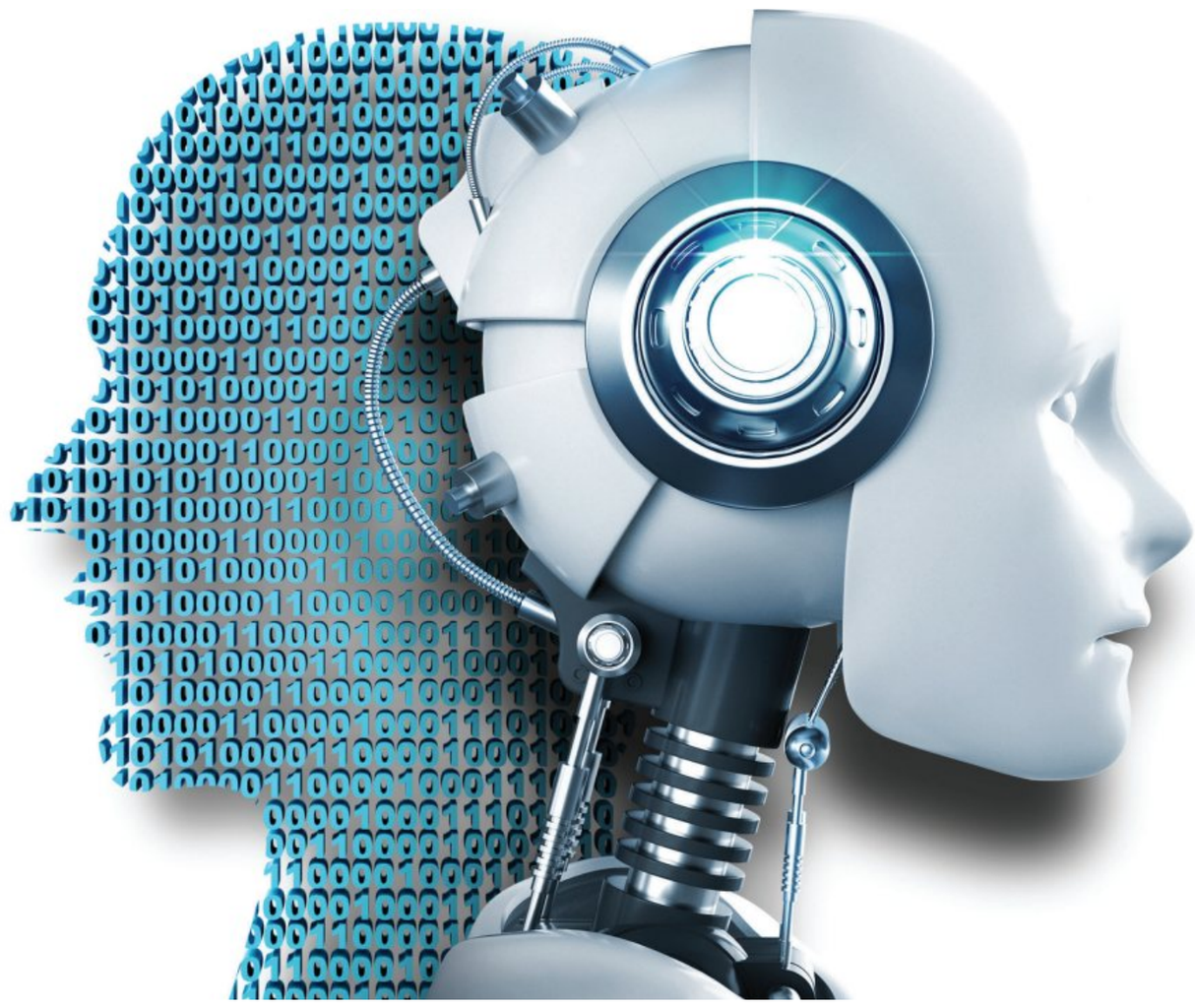
양자 컴퓨터 '보안 경보'… 국제 표준 암호 만든다

김영식 조선대 교수 등 6개 대학 공동 연구팀 개발 나서

한국형 양자 내성 암호 '동형암호' 알고리즘 안정화 성과



기존 컴퓨터와 궤를 달리하는 신기술 컴퓨터, '양자 컴퓨터'의 발전에 '보안 경보'가 울리고 있다.

지난 2019년 구글이 슈퍼 컴퓨터를 능가하는 양자 컴퓨터를 개발했다고 발표한 데 이어 인텔이 128큐비트 양자칩까지 개발하면서 양자 컴퓨터 발전이 더욱 빨라지고 있다.

마냥 희망찬 이야기만은 아니다. 양자 컴퓨터는 공인인증서부터 국가 기밀까지, 인터넷에 유통되는 모든 암호화된 정보들을 '무장 해제'시킬 수 있어 보안 위협도 높이고 있기 때문이다.

세계적으로 새로운 보안 시스템인 '양자 내성 암호' 연구에 불이 붙었다. 우리나라도 예외는 아니다. 조선대 김영식 교수와 서울대 노종선 교수, 한양대 신동준 교수, 동국대 임대운 교수, 대구경북과학기술원 김용준 교수, 공주대 서창호 교수가 힘을 합쳐 양자 내성 암호 개발에 힘쓰고 있다.

김영식 교수는 "양자 컴퓨터는 성능과 별개로, 태생적으로 기존 공개키 암호들을 마음대로 해독할 수 있는 특성을 갖고 있다"며 "양자 컴퓨팅 환경에 맞는 강력한 암호화 시스템이 시급하다"고 말했다.

지난 2017년 공개된 2000큐비트 양자 컴퓨터 'D-웨이브 2000Q'. 〈D wave 웹사이트 갈무리〉

◇기존 컴퓨터와 180도 다른 양자 컴퓨터

양자 컴퓨터는 양자 역학의 원리를 이용해 자료를 처리한다. 기존 컴퓨터의 기본 정보 단위는 '비트'(bit)로, 0 또는 1 둘 중 하나의 값을 가진다. 하지만 양자 컴퓨터의 정보 단위인 '큐비트'(Qubit)는 0과 1의 상태를 동시에 가질 수 있다. 양자 컴퓨터는 정보를 직접 관측하기 0인지 1인지 확정지을 수 없는 상태로 계산을 수행하기 때문이다.

1큐비트가 0과 1, 2개의 상태를 동시에 가지므로, 1개 값만을 가진 1비트에 비해 2배 빠른 계산이 가능하다. 2큐비트는 00, 01, 10, 11 4개 상태를 동시에 가져 2비트보다 4배 빠르며, 3큐비트는 8배, 4큐비트는 16배로 늘어난다. 처리 가능한 큐비트 양이 늘어날수록 정보 처리 속도가 기하급수적으로 빨라지는 것이다.

양자 컴퓨터는 당초 불확실한 정보를 바탕으로 계산을 하는 만큼 계산 결과도 여러 가지로 나오며, 이 중 최적의 답을 찾아낸다. 예컨대 A에서 B까지 가는 길을 찾고자 할 때, 양자 컴퓨터는 가능한 모든 경로를 동시에 찾아본 뒤 그 중 가장 일찍 도착한 경로를 답으로 제시한다. 한 번에 1가지 경로씩 일일이 계산해야 하는 기존 컴퓨터보다 훨씬 빠른 계산 방법이다.

◇발전하는 기술, 커지는 위협

양자 컴퓨터는 학문적인 용도나 많은 연산량이 필요한 빅데이터, 인공지능(심층신경망), 시장 분석, 암호 해독, 등에 유용하다고 알려졌다.

이 중 양자 컴퓨터의 암호 해독 능력에 대비하는 게 급선무다.

현재 전세계에서 가장 보편적으로 쓰이는 보안 방식중 하나는 '공개키' 암호화 방식이다. 공인인증서부터 인터넷뱅킹, 'https' 등 웹 보안 프로토콜, 비트코인 등 인터넷 전반에서 쓰이고 있다.

공개키 방식은 '소인수분해'와 '이산 로그' 문제를 바탕으로 암호화를 진행한다. 기존 컴퓨터로 이 문제를 풀려면 수십억년이 넘는 시간이 필요해 강력한 보안 시스템으로 활용됐다.

문제는 '소인수분해'와 '이산 로그' 모두 양자 컴퓨터가 특히 강한 분야라는 점이다. 소인수분해를 가장 빠르게 할 수 있는 양자 알고리즘인 '쇼어 알고리즘'을 수행할 수 있다는 점이 대표적이다. 이는 기존 컴퓨터에서는 작동하지 않는 알고리즘이다.

김 교수는 "3000큐비트 양자 컴퓨터가 개발되는 시점에서 현재 가장 비트 수가 높은 암호화 알고리즘인 'RSA2048'도 무력화된다"며 "학계에서는 2023년께에 1000큐비트 양자 컴퓨터가 등장할 것으로 보고 있다. 그 이전에 양자 내성 암호를 활성화해야 한다"고 설명했다.

◇한국형 '양자 내성 암호' 개발에 앞장

국제사회에서는 최근 국제 표준으로 삼을 양자 내성 암호를 찾고 있다.

미국국립표준기술연구소(NIST)는 지난 2016년 포스트 양자 알고리즘 표준화를 위한 알고리즘 제안 요청을 공지했다. 이듬해에는 82개 알고리즘을 접수하며 본격적으로 표준화 과정을 진행하기 시작했다. 양자 내성 암호는 다변수이차식 암호, 격자 기반 암호, 부호 기반 암호, 해시 기반 암호 등이 연구되고 있다.

김 교수는 지난해 11월 공동연구를 진행해 양자 내성 암호 중 하나인 격자 기반 '동형암호' 알고리즘을 안정화하는 첫 걸음을 뗐다.

동형암호는 정보를 암호화된 상태로 계산을 할 수 있게 하는 암호화 기법이다. 기존 동형암호는 1~2차례만 연산을 진행해도 오류가 심해 활용도가 떨어졌으나, 김 교수 연구팀은 오류를 줄이는 '부트스트래핑' 기법을 정밀화해 연산 가능 횟수를 1000배 이상 증가시켰다. 이 성과는 암호 분야 세계 최고 양대 학술대회 중 하나인 '유로크립트 2021'에서 발표됐다.

조선대 김영식(맨 뒤) 교수와 연구팀이 양자 컴퓨터의 암호 해독 능력을 방어하는 양자 내성 암호를 개발하고 있다. 〈김영식 교수 제공〉

연구팀은 동형암호뿐 아니라 국제 경쟁력을 갖춘 다양한 양자 내성 암호 설계 및 분석, 구현할 수 있도록 연구를 거듭하고 있다. 향후 국내 연구자들이 격자 기반 암호, 완전 동형 암호 등 최신 기술을 쉽게 습득하고 지속적인 암호 연구를 이어갈 수 있도록 기반을 마련하는 것도 연구팀의 역할이다.

김 교수는 "국내에서도 표준적인 양자 내성 암호 기술을 만드는 데 앞장서겠다. 미래에 꼭 필요한 암호 기술들을 우리 힘으로 고도화시키고, 나아가 https처럼 세계적으로 쓰이는 국제 표준 암호안까지 만드는 것이 목표다"고 말했다.

/유연재 기자 yjyou@kwangju.co.kr