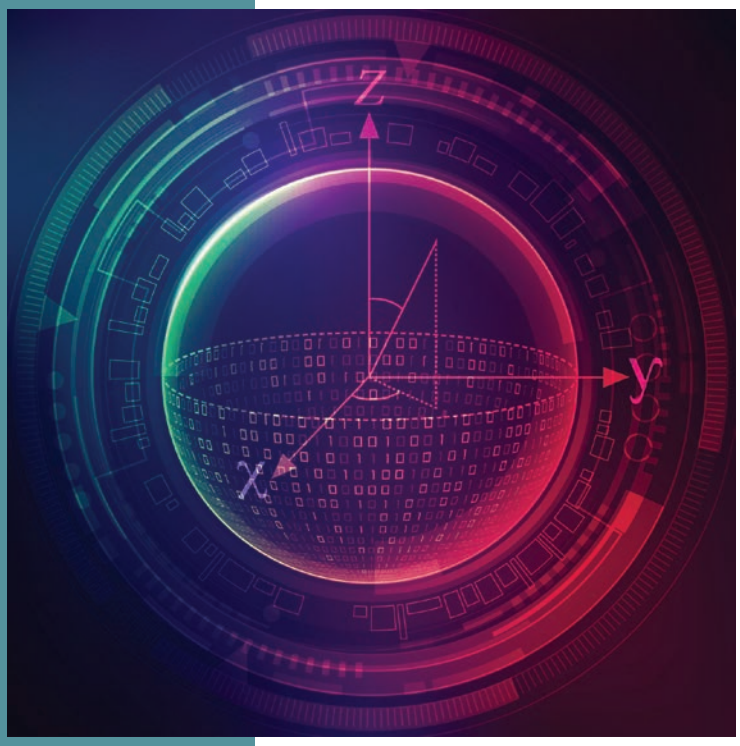
양자 시대의 데이터 보안



©Getty

웹사이트에 로그인하거나 전자우편을 보내거나 온라인 구매를 할 때마다, 해커들이 암호를 깰 수 없을 정도로 데이터가 안전하게 전송된다는 것에 의지합니다. 표준 암호 시스템은, 예를 들어 매우 큰 수의 소인수들을 찾는 일처럼 현재의 컴퓨터가 쩔쩔매는 수학 문제들에 전적으로 의존하고 있습니다. 하지만 다가올 수십 년 내에는 이런 문제 몇 가지를 강력한 양자 컴퓨터가 빠르게 풀어내어, 온라인 통신의 안전성을 위협할 것으로 예상하고 있습니다. 가장 정교한 양자 컴퓨터에도 견딜 수 있는 새로운 방법들을 개발하기 위해, 암호학자들은 다양한 범위의 수학 도구(원래는 실생활 응용을 염두에 두지 않고 개발됐던 도구)들을 이용합니다.

미국 국립 표준 기술 연구소 NIST는 미래의 양자 시대에 데이터를 지키기 위한 알고리즘, 즉 단계별 절차를 표준화하려는 노력을 선도하고 있습니다. NIST 연구자들은 제안된 알고리즘 수십 개의 보안, 속도, 비용 등을 테스트하고 있습니다. 고차원 격자, 선형 오류 정정 부호, 타원 곡선 사이의 등원성(isogeny) 등의 수학이 관련돼 있습니다. 문서의 진위를 검증하는 디지털 서명, 누구나 메시지를 보낼 수 있지만 받아야 할 사람만이 읽을 수 있게 하는 공개 키 암호화, 암호화 및 복호화에 이용되는 암호 키 생성에서, 양자 컴퓨터에 가장 잘 견디는 알고리즘을 가려내는 것이 NIST의 목표입니다. 그럼으로써 암호학자들은 이런 알고리즘의 표준 버전들을 개발할 수 있을 것입니다. 다가올 몇 년 동안 새로운 양자 내성 암호들이 정부 컴퓨터부터 여러분 주머니 속의 휴대전화까지 모든 곳에서 오늘날의 보안 시스템을 점차 대체해 갈 것입니다.

더 알아보기: "How the United States Is Developing Post-Quantum Cryptography" by Jeremy Hsu, *IEEE Spectrum*, September 6, 2019.

Translation courtesy of the Korean Mathematical Society

Watch an interview with an expert!

MM/158/KR

AMS
AMERICAN MATHEMATICAL SOCIETY

Mathematical Moments *프로그램은 과학, 자연, 기술, 그리고 인간의 문화에서 수학이 하는 역할에 대한 올바른 평가와 이해를 촉진합니다.*

www.ams.org/mathmoments