컴퓨터의 변혁 일으키기

20여 년 안에 컴퓨터 칩이 너무 작아져서 양자역학의 효과들이 우리가 당연시했던 물리법칙을 대체할 것입니다. 오늘날 우리가 사용하는 컴퓨터는 0이거나 1인 비트를 토대로 하지만, 양자계산의 기본 단위는 동시에 (각각에 확률이 부여된) 0과 1이 될 수 있는 양자 비트(큐비트)입니다. 양자계산이라는 이상한 세상에서는 큰 숫자를 인수분해하는 것과 같은 복잡한 과정도 관련된 여러 단계를 동시에 계산할 수 있기 때문에 훨씬 빠른 속도로 이뤄집니다. 이 분야를 연구하는 수학자, 물리학자, 컴퓨터 과학자와 공학자들의 궁극적인 목표는 오늘날의 가장 강력한 컴퓨터로도 수십억 년이 걸리는 문제들을 몇 초 안에 풀 수 있는 양자 컴퓨터를 만드는 것입니다.

양자 컴퓨터의 능력에는 오늘날의 전자 암호 방법을 깰 수 있는 계산능력도 포함됩니다. 이것은 들리는 만큼 그리 걱정스러운 일은 아닌데, 왜냐하면 암호학자들이 이미 시스템을 관찰하면 그 시스템이 변한다는 양자역학의 원리를 이용한 알고리즘을 개발했기 때문입니다. 그리하여, 양자 통신망을 사용하는 이용자들은 통신을 가로채려는 어떠한 시도도 감지할 수 있습니다. 오늘날에는 컴퓨터를 소형화하는 데 장벽으로 작용하는 법칙들이 미래에는 컴퓨터 사용에 큰 도움을 제공할 수도 있다는 사실은 아이러니입니다.

더 알아보기: "Rules for a Complex Quantum World," *Scientific American,* November 2002, Michael A. Nielsen.

Translation courtesy of volunteer members of the Korean Mathematical Society.

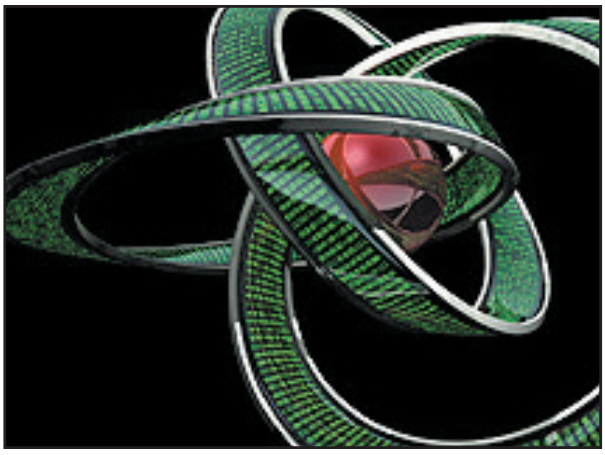

Image courtesy of the MITRE Corporation.