양자 알고리즘, 인터넷 암호화 해킹 속도 향상

(2023.09.22., 양자정보연구지원센터)

□ 효율적인 양자 소인수분해 알고리즘 발견

○ 큰 숫자를 인수분해하는 것은 Shor 알고리즘보다 효율적일 수 있음

- n 비트 정수는 양자 회로를 독립적으로 실행하여 인수분해할 수 있음
- 양자 컴퓨터로 인터넷 암호화 체계를 해킹하려면 수백만 또는 수십억 큐비트가 필요할 수 있음

○ P. Shor 양자 컴퓨터 최초 실제 용도 중 하나인 인터넷 해킹 창안(1994)

- 양자 컴퓨터가 큰 숫자의 소인수를 찾는데 고전 컴퓨터보다 기하급수적으로 빠른 방법을 보여줌, Shor 알고리즘은 양자 컴퓨터의 가능성을 보여주는 예로 지속됨
- 이러한 소인수는 인터넷을 통해 전송되는 대부분의 암호화된 정보 보호에 비밀 키를 사용됨

○ 더 나은 양자 알고리즘 공개(뉴욕 대학 O. Regev, arXiv 공개)

- 매우 큰 숫자를 인수분해하는 데 필요한 게이트 수 또는 논리적 단계를 크게 줄일 수 있는 체계 제안
- 원칙적으로, 더 작은 양자 컴퓨터가 비밀 암호화 키를 찾아내거나 더 큰 기계가 이를 더 빨리 해독할 수 있도록 함

○ Shor 알고리즘과 Regev 알고리즘 비교

- 모든 양자 알고리즘과 마찬가지로, 0과1 뿐만 아니라 동시에 0과 1의 “중첩”으로 설정될 수 있는 양자 비트 또는 큐비트의 신비한 특성에 의존함
- 이러한 큐비트 중 소수는 알고리즘의 논리적 작업 수행에 게이트로 함께 연결될 수 있음, n비트 길이 숫자를 인수분해하려면 n^2 **게이트의 양자 회로가 필요**함
- 대부분 인터넷 암호화는 최소 2048비트 숫자에 의존(617자리 십진수),

Shor 알고리즘을 사용하여 소인수를 찾으려면 최소 400만 개의 게이트가 있는 양자 컴퓨터가 필요함

- 환경 노이즈는 큐비트의 섬세한 중첩 상태를 파괴, 오류 수정을 통해 잡음 해결할 수 있지만, 훨씬 더 많은 큐비트(수백만 또는 수십억)가 필요함

- Shor 알고리즘은 1D, 단일 숫자를 높은 거듭제곱으로 올려 소인수 검색, 결과에 도달하기 전 많은 큰 숫자를 함께 곱해야 함
- Regev, 다양한 차원에서 여러 숫자를 곱할 수 있음을 발견
- 두 알고리즘은 거의 동일한 총 곱셈 횟수를 요구하지만, Regev 다차원 특성은 결과에 도달하기 전에 곱해진 숫자가 그만큼 커지지 않음
- n 비트 정수를 인수분해하는 데 $n^{1.5}$ **게이트만 필요**하다는 것을 발견
- 그 구조는 계산 중 중간 값을 저장하기 위해 양자 메모리가 필요하며, 이는 까다로운 큐비트가 더 많이 필요함을 의미함, 알고리즘 비용 상승

ㅇ 양자 컴퓨터가 Regev 또는 Shor 알고리즘을 구현하여 소인수를 찾을 준비가 되면 인터넷 암호화가 진행되었을 수 있음

- 보안 지도자들은 이미 양자 해킹에 면역이 될 "격자 암호화(lattice cryptography)" 포함한 대안으로 전환하고 있음
- 그럼에도 Regev 연구의 참신함이 획기적 발전을 위해 애쓰고 있는 양자 암호화 분야에서 다른 새로운 아이디어에 영감을 주고 생성할 가능성이 있음

(원문)

1. https://www.science.org/content/article/surprising-and-supercool-quantum-algorithm-offers-faster-way-hack-internet-encryption