아마존 연구자, 양자 알고리즘이 PQC의 기반에 도전할 가능성 제기

(2026.09.10., 양자정보연구지원센터)

□ **아마존 연구자, 새로운 양자 알고리즘 제안, 격자 기반 PQC 핵심 수학적 가정에 새로운 도전 제기**

○ Amazon 연구자, 격자 기반 양자내성암호(PQC)의 수학적 기반에 도전하는 양자 알고리즘 제시

- Amazon Web Services(AWS) 암호학 연구자 Daniel R. Simon은 20년 이상 연구돼 온 “Dihedral Coset Problem(DCP)”에 대해 다항시간(polynomial-time) 양자 알고리즘을 제안

- DCP는 특정 격자 문제와 연관되어 있어, 해당 알고리즘이 검증될 경우 **격자 기반 암호의 안전성에 대한 기존 가정에 중요한 영향을 줄 가능성**이 있음

- 특히 DCP 알고리즘을 기존의 이론적 환원 기법과 결합하면 “Shortest Vector Problem(SVP) 및 Learning With Errors(LWE)”의 일부 근사 문제를 양자컴퓨터로 다항시간에 해결할 수 있다는 결과를 제시

○ **PQC 전체가 즉시 해킹되는 것은 아니며, 아직 이론적 연구 단계**

- SVP와 LWE는 NIST가 표준화한 다수의 **양자내성암호(PQC) 알고리즘의 핵심 수학적 기반**으로 활용되고 있음

- 그러나 이번 연구는 특정 암호 표준에 대한 실제 공격이나 암호키 복구를 수행한 것이 아니라, 관련 수학 문제가 기존 예상보다 **양자컴퓨터에서 훨씬 효율적으로 풀릴 수 있음을 이론적으로 제시**

- 실제 암호체계에 적용하려면 암호학적 파라미터, 논리 큐비트 수, 양자 게이트 수, 오류정정 등 **현실적인 계산 자원과 공격 가능성에 대한 추가 분석**이 필요

○ **기존 DCP 알고리즘의 한계를 극복하는 새로운 접근 제시**

- 기존의 대표적인 양자 알고리즘은 준지수(subexponential) 시간에 동작했으며, 다항시간 알고리즘은 확보되지 않았음

- Simon은 기존 연구에서 사용된 이상적인 Subset-Sum Oracle 없이 양자 샘플을 여러 그룹으로 나누고 불필요한 정보를 제거하는 새로운 방법을 제안
- 또한 일부 오류가 포함된 입력 샘플을 처리할 수 있도록 설계해, 관련 격자 문제로의 이론적 환원 가능성을 높였다고 주장

○ 향후 독립적인 검증이 핵심

- 논문의 핵심은 양자 상태에서 필요한 정보를 보존하면서 오류와 위상 정보를 제거하는 과정이 실제로 제시된 확률적·수학적 조건을 만족하는지 여부
- 특히 확률적 경계와 재귀적 계산 과정, 실제 양자 회로로 구현했을 때의 계산 복잡도 등에 대한 **전문가들의 면밀한 검증이 필요**
- 현재는 프리프린트 단계이므로, 연구 결과가 검증될 경우 **양자 알고리즘 및 PQC 연구에 상당한 영향을 미칠 수 있지만, 현 시점에서 기존 PQC가 무력화됐다고 판단하기는 어려움**

○ **PQC 표준 및 양자암호 연구에 미칠 잠재적 영향**

- 이번 결과가 독립적으로 검증되고 실제 암호학적 파라미터까지 확장될 경우, 현재 널리 활용되는 **격자 기반 PQC의 안전성 가정과 파라미터 설정을 재검토해야 할 가능성**이 있음
- 특히 LWE·SVP와 같은 수학적 난제에 대한 양자 알고리즘의 발전은 향후 새로운 공격 기법으로 이어질 수 있어, **PQC 표준에 대한 지속적인 암호분석과 대체 후보 기술 확보가 중요**해질 전망
- 다만 현재 연구는 특정 표준 암호를 직접 공격한 결과가 아니며, 실제 암호체계에 적용 가능한 수준의 양자 하드웨어 및 계산 자원이 제시된 것도 아니므로 **'PQC가 깨졌다' 기보다는 향후 보안 가정에 대한 중요한 경고 신호**로 보는 것이 적절함

(원문)

1. https://thequantuminsider.com/2026/08/06/amazon-researcher-claims-quantum-algorithm-could-challenge-pqc-foundations/