Q-Day, IBM 연구팀 하이브리드 Quantum-AI 단기적 위협 초래

(2024.03.27., 양자정보연구지원센터)

□ **양자 컴퓨터와 인공 지능의 결합이 현재의 암호화 방법을 약화시킬 위험이 있음**

○ 하이브리드 양자-고전 컴퓨팅(hybrid quantum-classical computing, HQCC)과 인공 지능(artificial intelligence, AI) 기술의 결합이 양자 컴퓨터가 현재 암호화 방법을 해독하는 시간을 빠르게 앞당길 수 있음

- 양자 컴퓨터가 현재 암호화 방법을 해독하는 데 충분히 강력하고 안정되어 있는 시기 "Q-day"
- 이러한 위험은 암호학 관련 전문가들에게 긴장감을 불러일으키고 있으며, 이에 대한 신속한 대응이 필요함

○ 기술의 발전은 긍정적인 측면 뿐만 아니라 위험도 동반함

- 양자 컴퓨팅과 인공 지능의 발전은 빠르게 진행되고 있으며, 이러한 발전은 암호화 방법을 약화시킬 수 있는 가능성을 내포하고 있음
- **ML(machine learning) 알고리즘으로 보완된 HQCC 프레임워크**가 특히 우려스러운 결과를 초래할 수 있다고 강조함
- 특히, 양자 알고리즘의 발전은 암호학에 새로운 도전을 제시할 수 있음, Grover 적응형 검색(Grover's Adaptive Search, GAS) 과 Harrow-Hassidim-Lloyd(HHL) 방법 등 양자 알고리즘이 암호화 해독에 지수적으로 효율적일 수 있음

- 한편, HHL 알고리즘은 일부 조건 하에 고전적 방법보다 지수적으로 빠르게 선형 방정식 체계를 해결하는 능력을 보였음, HHL의 수학적 능력은 **양자 견고한(quantum-resistant) 암호화**의 주요 후보 중 하나인 **격자 기반(lattice-based)** 암호화의 보안 기초를 약화시킬 수 있음
- 예를 들어, 새로운 알고리즘은 격자 기반 시스템의 보안에 중요한 노이즈가 있는 선형 방정식을 다루는 데 능숙해질 수 있음

ㅇ 이에 대응하여, 암호학 및 보안 분야 전문가들은 양자 견고한 암호화 방법의 개발과 적용을 위한 노력을 강화해야 함

- 더욱이, 인공 지능과 기계 학습 기술이 함께 사용될 경우, 암호 분석에 더 큰 위험을 초래할 수 있음
- **"AI 주도 암호 분석(AI-driven cryptanalysis)"** 은 검색 알고리즘을 최적화하고 미묘한 취약점을 찾아내어 암호화 표준의 약점을 가속화 할 수 있음
- 이러한 기술 발전은 PQC(Post-Quantum Cryptography) 이주 시간표에도 영향을 미치며, 양자 미래에 대비하여, 정부, 산업 및 학계는 양자 컴퓨팅의 수학적 이점을 이기는 암호화 방법 개발을 위해 협력, 가속화 필요성 주장

ㅇ IBM 연구팀은 이러한 위협을 강조, 암호화 표준화의 가속화, HQCC 개발의 지속적인 모니터링, 새로운 후속 양자 암호학 연구에 대한 투자를 권장하고 있음

- 이러한 대응 조치는 현재 암호화 방법을 보호하고 양자 컴퓨팅의 영향을 최소화하는 데 필요함

ㅇ 양자 컴퓨팅 및 AI 발전이 **PQC migration** 일정에 미칠 영향 가능성

- 하이브리드 양자-고전 컴퓨팅, 인공 지능(AI), 기계 학습(ML), 딥러닝(DL)의 발전은 암호화에 심각한 위협을 제공할 수 있음
- 기술적 융합은 암호화 공격을 더욱 효율적으로 만들 수 있는 그로버의 적응형 검색(GAS)과 양자 가속화 HHL 알고리즘을 검토함
- 이러한 위험에 대비하기 위해 양자 견고한 AI/ML 암호화 솔루션의 개발 및 적용에 대한 적극적인 접근이 필요함

(원문)

1. https://thequantuminsider.com/2024/03/26/is-q-day-closer-than-we-think-ibm-researchers-say-hybrid-quantum-ai-may-poses-near-term-threats/