양자 컴퓨팅, 장기적 사이버 보안 위협, 즉각적 대응 필요

(2025.02.20., 양자정보연구지원센터)

□ **양자 컴퓨팅은 장기적인 사이버 보안 위협이지만, 즉각적인 대응이 필요하다고 분석가들은 보고함**

○ 개요, MITRE 보고서

- 양자 컴퓨터가 고급 보안 암호를 해독할 수 있는 능력을 갖추기까지는 수십년이 걸릴 것으로 예상됨
- 그러나 미 정부 및 정보기관은 적대 세력이 양자 기술의 발전을 활용할 가능성에 대비해 지금부터 대응해야 한다고 경고함

○ **양자 컴퓨팅과 국가 안보**

- 해당 보고서는 주로 정보기관(IC)을 대상으로 작성됨
- 현재 RSA-2048 암호화 키는 적어도 수십 년 동안 안전할 것으로 예상되지만, 양자 컴퓨팅 기술의 예기치 않은 발전이 있을 경우 이보다 빠르게 해독될 가능성이 있음
- 보고서는 중국을 비롯한 경쟁국들이 이미 양자 기술을 활용한 암호 해독을 대비하고 있다고 지적함

○ 중국의 양자 기술 발전

- 현재 미국이 양자 컴퓨팅 분야를 주도하고 있지만, 중국도 빠르게 따라오고 있음
- 중국은 양자 통신 및 암호 키 분배 등의 관련 기술에서 상당한 진전을 이루었으며, 이는 향후 양자 컴퓨터 개발에서 우위를 점할 가능성이 있음
- 중국이 미국보다 먼저 양자 컴퓨터를 개발하지 못하더라도, 현재 수집한 암호화된 정보를 향후 해독할 수 있는 능력 확보 가능

○ 양자 컴퓨팅 발전 측정

- MITRE 연구진은 양자 컴퓨팅 발전을 평가하기 위해 IBM이 개발

한 **‘양자 볼륨(Quantum Volume, QV)’이라는 지표를 사용**함

- QV는 큐비트 개수와 오류 없는 계산 수행 능력을 함께 고려하는 방식으로 양자 컴퓨팅 성능을 측정함
- 보고서는 현재의 발전 속도를 고려할 때, RSA-2048 암호를 해독할 수 있는 양자 컴퓨터가 2055~2060년 이전에 등장할 가능성은 낮다고 분석함
- 그러나 일부 전문가들은 낙관적인 전망을 내놓으며, 양자 오류 수정 및 알고리즘 설계의 발전에 따라 2035년까지 암호 해독이 가능할 수도 있다고 주장함

○ 양자 컴퓨터의 광범위한 영향

- 보안 위협 외에도 양자 컴퓨팅은 다양한 산업에서 혁신을 가져올 것으로 기대됨
- 특히 소재 과학, 제약, 인공지능(AI) 등의 분야에서 획기적인 발전을 이끌어낼 가능성이 있음
- 물류, 공급망 관리, 국방 분야에서도 최적화 문제를 기존 슈퍼컴퓨터보다 훨씬 빠르게 해결할 수 있어 전략적 가치를 가짐
- AI 분야에서는 소규모 데이터셋을 활용한 학습 속도 향상 및 정확도 증가 효과를 기대할 수 있음

○ **포스트 양자 암호(PQC) 도입의 시급성**

- 대규모 양자 컴퓨터가 등장하려면 수십 년이 걸릴 것으로 예상되지만, MITRE 보고서는 미국 정부가 지금부터 포스트 양자 암호(PQC) 로 전환을 준비해야 한다고 강조함
- 이는 미국 국립표준기술연구소(NIST) 및 국가안보국(NSA)이 진행 중인 양자 내성 암호 표준 개발 움직임과 일맥상통함
- 연구진은 정보기관(IC)이 양자 컴퓨터 위협으로부터 기밀 데이터를 보호하고, 양자 컴퓨팅의 발전을 지속적으로 모니터링해야 한다고 강조함
- 적대 세력이 현재 암호화된 통신을 저장해 두었다가, 향후 양자 컴퓨터가

등장하면 이를 해독하는 전략을 사용할 가능성이 있기 때문임(“harvest now, decrypt later”)

ㅇ 전략적 투자 필요성

- MITRE 보고서는 보안뿐만 아니라 기술적 우위를 확보하기 위해 지속적인 양자 연구 투자가 필요하다고 주장함
- 현재 미국이 양자 기술을 선도하고 있지만, 향후 중국을 비롯한 다른 국가들이 빠르게 따라올 가능성 잇음
- 따라서 글로벌 양자 기술 동향을 면밀히 모니터링하고, 국가 차원의 전략적 대응이 필요함
- 특히, 양자 기술의 핵심 부품(예: 극저온 냉각기, 레이더 등)의 공급망을 확보하여 외국 의존도를 줄이는 것이 중요함

ㅇ 향후 전망 및 대응 방안

- 보고서는 양자 컴퓨터가 암호를 해독할 수 있는 시점이 아직 멀었지만, 정보기관이 미리 대비해야 한다고 강조함
- 이를 위해 다음과 같은 세 가지 핵심 대응책을 제안함
- 포스트 양자 암호(PQC)로의 전환을 가속화하여 민감한 정보 보호
- 적대국의 양자 연구 프로그램을 면밀히 감시하여 예상치 못한 기술 발전에 대비
- 양자 연구 및 공급망 보안을 강화하여 미국이 기술적 주도권을 유지할 수 있도록 함

ㅇ MITRE는 정부와 민간 부문이 협력하여 양자 기술 발전을 모니터링하고, 보안 및 기술 리더십을 유지해야 한다고 주장함

- 양자 컴퓨터가 보안에 미칠 영향을 최소화하기 위해서는 신속하고 전략적인 대응이 필수적임

(원문)

1. https://thequantuminsider.com/2025/02/01/quantum-computing-is-a-long-term-cybersecurity-risk-but-deserves-immediate-attention-analysts-report/