# NIST, 최초 3개 최종화된 포스트 양자 암호화 표준 출시 공식 발표

(2024.09.10., 양자정보연구지원센터)

## □ NIST, 양자 컴퓨터 대응 암호화 알고리즘 발표

○ 미 상무부 산하 국립표준기술연구소(NIST)가 양자 컴퓨터 공격에 견딜 수 있는 암호화 알고리즘 세트를 발표함

- 해당 알고리즘은 NIST의 **'양자 후 암호화(PQC) 표준화 프로젝트'**의 결과물로, 즉시 사용 가능함
- 양자 컴퓨터가 현존하는 암호화 기술을 무력화할 수 있는 가능성에 대응한 조치임

○ 전 세계 연구진들이 양자 컴퓨터 개발에 박차를 가하고 있으며, 이 기술이 기존 컴퓨터와 매우 다른 방식으로 작동할 것이라고 예상됨

- 일부 전문가들은 양자 컴퓨터가 향후 10년 내에 등장할 수 있으며, 이는 현재의 보안 시스템을 위협할 수 있다고 경고함
- 양자 컴퓨터는 현재의 암호화 방법이 해결하기 어려운 수학적 문제를 빠르게 해결할 수 있기 때문에, 현존하는 암호화 방식을 무력화할 가능성이 있음

○ **양자 컴퓨터의 위협과 NIST의 대응**

- NIST가 발표한 새로운 암호화 표준은 양자 컴퓨터의 위협을 대비한 것임
- 발표된 알고리즘은 복잡한 수학적 문제를 기반으로 하여, 양자 컴퓨터와 기존 컴퓨터 모두에 대해 안전성을 보장함
- NIST는 8년간의 연구 끝에 이 알고리즘을 개발했으며, 전 세계 암호 전문가들이 참여함

○ NIST는 양자 컴퓨터가 날씨 예측, 기초 물리학, 약물 설계 등 다양한

분야에서 혁신을 일으킬 수 있다고 전망함

- 하지만, 이러한 기술 발전이 보안과 프라이버시에도 심각한 위협을 가할 수 있음
- NIST는 이를 대비하기 위해 포스트-양자 암호화(PQC) 기술을 개발 중임

ㅇ 새로운 암호화 표준의 주요 내용

- 이번에 발표된 표준에는 **암호화 알고리즘의 컴퓨터 코드, 구현 방법, 사용 목적 등이 포함**되어 있음
- 이 표준은 향후 양자 컴퓨터의 등장에 대비하여, 일반적인 암호화와 디지털 서명을 보호하기 위한 도구로 사용됨
- NIST는 시스템 관리자들이 새로운 알고리즘을 시스템에 통합하기 시작해야 한다고 권고함

ㅇ 백업 알고리즘 평가 진행

- NIST는 추가적으로 두 가지 알고리즘 세트를 평가하고 있으며, 이들이 미래의 백업 표준으로 사용될 가능성이 있음
- 첫 번째 세트는 **일반적인 암호화**를 위한 것으로, 이번에 발표된 표준과는 다른 수학적 문제를 기반으로 함
- 두 번째 세트는 **디지털 서명을 보호**하기 위한 것으로, NIST는 2022년에 추가 알고리즘을 공개 모집하여 평가 중임

ㅇ 양자 컴퓨팅 기술과 보안의 미래

- NIST는 이번 표준이 양자 컴퓨터가 사회에 미칠 영향을 고려한 중요한 단계라고 설명함
- 이번에 발표된 표준은 양자 컴퓨팅 기술이 사회적 문제를 해결할 수 있도록 하면서도, 보안을 유지하기 위한 NIST 노력을 상징함
- NIST는 추가 알고리즘에 대한 분석을 계쏙 진행하면서, 백업 계획을 마련할 것임

○ **양자 컴퓨터 도입을 위한 준비 권고**

- NIST는 시스템 관리자들이 즉시 새로운 암호화 알고리즘을 통합해야 한다고 강조함
- 양자 컴퓨터가 현재 암호화 시스템을 무너뜨릴 가능성이 있는 만큼, 대비책이 시급함
- “미래의 공격에 대비하여 이번에 발표된 세 가지 표준을 우선적으로 사용해야 한다”고 권고함

○ 양자 보안에 대한 다양한 의견

- 양자 보안 전문가들은 이번 NIST 발표를 역사적인 순간으로 평가하며, 모든 산업 분야에서 보안 시스템을 현대화해야 한다고 주장함
- 영구 사이버 보안 회사 PQShield의 CEO는 “양자 보안을 위한 기술 도입이 시급하다”고 언급하며, 이번 발표가 전 세계적인 보안 전환의 시작이라고 평가함
- 또 다른 전문가들은 양자 컴퓨팅이 보안에 위협이 될 수 있는 동시에, 미래 기술을 선도할 것이라는 기대를 내놓음
- 각 산업의 보안 책임자들은 새로운 암호화 표준을 도입하여 시스템을 강화해야 한다고 강조함

**(원문)**

1. https://thequantuminsider.com/2024/08/13/nist-officially-announces-release-of-first-3-finalized-post-quantum-encryption-standards-plus-quantum-community-reaction/