NIST, 9개 포스트양자 전자서명 알고리듬 3차 평가 단계 진출

(2026.06.09., 양자정보연구지원센터)

□ NIST, 차세대 포스트양자 전자서명 알고리듬 9종, 3차 심사 대상 선정

○ NIST, 포스트양자 전자서명 알고리듬 9종 3차 평가 단계 선정

- 미국 National Institute of Standards and Technology(NIST)는 포스트양자암호(PQC) 추가 전자서명 표준화 과정에서 9개 후보 알고리듬을 3차 평가 단계로 선정함
- 선정된 알고리듬은 FAEST, HAWK, MAYO, MQOM, QR-UOV, SDitH, SNOVA, SQIsign, UOV 등 총 9종임
- 약 18개월간의 평가를 거쳐 선정되었으며, 향후 약 2년간 추가 검증과 개선 작업이 진행될 예정임

○ **포스트양자 전자서명**의 중요성

- 전자서명은 사용자 인증, 소프트웨어 업데이트 검증, 금융거래 보호, 데이터 무결성 확인 등 현대 사이버보안의 핵심 기술임
- 양자컴퓨터가 충분한 규모로 발전할 경우 현재 널리 사용되는 공개키 암호체계가 해독될 가능성이 제기되고 있음
- 이에 따라 양자컴퓨터 공격에도 안전한 새로운 전자서명 기술 확보가 국가 및 산업계의 주요 과제로 부상하고 있음

○ NIST 포스트양자암호 표준화 추진 현황

- NIST는 2016년부터 포스트양자암호 표준화 프로젝트 추진해 왔음
- 기존 표준화 과정에서는 CRYSTALS-KYBER(ML-KEM), CRYSTALS-Dilithium(ML-DSA), FALCON(FN-DSA), SPHINCS+(SLH-DSA) 등이 최종 표준으로 선정됨
- 이들 알고리듬은 대부분 격자암호(Lattice-Based Cryptography)에 기반하고 있음

○ **암호학적 다양성(Cryptographic Diversity) 확보 목적**

- NIST는 특정 수학적 가정에 과도하게 의존하는 위험을 줄이기 위해 추가 전자서명 프로젝트를 추진함
- 미래에 특정 암호체계의 취약점이 발견될 경우 신속하게 대체할 수 있는 '암호 민첩성(Cryptographic Agility)' 확보가 중요해지고 있음
- 이에 따라 격자 기반이 아닌 다양한 수학적 원리에 기반한 후보군 확보를 목표로 하고 있음

○ **후보 알고리듬의 특징**

- 2022년 NIST는 다양한 포스트양자 전자서명 기술 제안을 공개 모집
- 총 40개 후보가 접수되었으며, 2023년 1차 평가를 시작으로 14개 후보가 2차 단계에 진출함
- 이번 평가를 통해 최종 9개 후보가 3차 단계에 선정됨
- 선정된 알고리듬들은 **다변수 암호(Multivariate Cryptography), 부호 기반(Code-Based Cryptography), 기타 새로운 대수학적 접근법 등을 활용**하고 있음
- 이는 격자 기반 암호와 다른 수학적 난제에 기반하여 장기적인 보안 다양성을 제공할 수 있음

○ 평가 기준 및 향후 일정

- NIST는 공개 검증 방식을 통해 학계, 정부기관, 산업계 전문가들의 평가를 받고 있음
- 보안성뿐 아니라 구현 효율성, 계산 성능, 부채널 공격(Side-Channel Attack) 저항성 등을 종합적으로 검토함
- 참여 연구팀은 향후 2년 동안 알고리듬 사양 및 구현 방식을 개선할 수 있음
- NIST는 2027년 미국 메릴랜드주 게이더스버그에서 제7회 포스트양자암호 표준화 컨퍼런스를 개최할 예정이며, 해당 회의가 차세

대 표준 선정의 주요 이정표가 될 전망임

ㅇ 결론

- 이번 3차 평가 단계 선정은 양자컴퓨터 시대를 대비한 차세대 전자서명 표준 확보 노력의 일환임
- 특히 기존 격자 기반 암호 외에도 다양한 수학적 기반의 알고리듬을 육성함으로써 암호체계의 장기적인 안정성과 유연성을 강화하려는 전략적 의미를 가짐
- 향후 평가 결과에 따라 일부 후보는 차세대 국제 포스트양자 전자서명 표준으로 채택될 가능성이 있음

(원문)

1. https://thequantuminsider.com/2026/05/21/nist-advances-nine-post-quantum-signature-algorithms-to-third-round/