KQC

Are you ready for the Quantum Threat?

KQC

KQC와 함께
Quantum Safe를 준비하십시오

Are you ready for the Quantum Threat?

양자내성 암호 알고리즘 (PQC)로 전환은 선택사항이 아닙니다. 또 바로 지금해야 합니다!

양자 컴퓨터의 발전은 RSA, ECC 등 기존 공개키 암호 알고리즘을 무력화할 수 있는 잠재력을 가지고 있습니다. (쇼어 알고리즘 기준) 쇼어(Shor) 알고리즘은 이산로그 및 소인수분해 문제를 빠르게 해결할 수 있어, 현대 디지털 보안의 근간을 위협할 수 있습니다. 또한 새로운 공격 유형(HNDL(Harvest Now, Decrypt Later) 공격은 현재 암호화된 데이터를 수집해 저장한 뒤, 미래의 양자 컴퓨터로 복호화하려는 전략으로 탐지가 어려우며, 장기적인 피해 유발할 수 있습니다. 또한 AI의 등장으로 자동화된 공격, 지능형 피싱, 딥페이크 기반 사기 등이 현실화되면서 사이버 공격의 증가와 고도화되고 있습니다.

KQC 양자 내성 암호 기반 HSM 솔루션

Quantum-Safe
Crypto-Agile
Hardware Security Modules

- 단순 재활용아닌 PQC기반의 새로운 설계
- 세계최초로 FIPS140-3 PQC 인증 진행
- 양자안전 신뢰루트 (Root of Trust) 확보
- 키저장 – 멀티파티션으로 키보호 가능
- Full CNSA2.0 알고리즘

Designed, manufactured, and assembled in Canada by Crypto4A

KQC 양자 내성 암호 기반 하드웨어 보안키

PQC HW Security Key

Quantum-Safe
Enterprise Attestation
Biometric Security Authentication

- 세계최초 PQC 하드웨어 보안키
- 지문인식기반으로 보안 강화
- ECDSA/Dilithium 하이브리드 가능
- 기업향 인증서 가능
- PUF (Physically Uncronable Function) 사용으로 보안제고

KQC 한국퀀텀컴퓨팅㈜

48058 부산광역시 해운대구 센터중앙로 55, 9층 | 06752 서울특별시 서초구 바우뫼로 27길 7-7, 6층
www.Kqchub.com