ISO, 양자 키 분배(QKD) 보안 표준 발표

(2023.09.08., 양자정보연구지원센터)

□ ISO(국제 표준화 기구), QKD 보안 요구 사항 전용 표준 확립

○ 기존 네트워크 구성 요소, 양자 광학 구성 요소 및 QKD 프로토콜 전체 구현 포함한 QKD 모듈 측면 다룸, QKD 개발을 위한 국제 표준

- 국제 표준화 기구(ISO, International Organization for Standardization)는 양자 키 분배(QKD, Quantum Key Distribution) 보안 요구 사항에 대한 최초의 표준 세트 도입, ISO/IEC 15408 시리즈에 따라 QKD 시스템의 보안 평가를 위한 포괄적 프레임워크 설명

○ 양자 암호화 분야의 중요한 움직임으로 인식하고 있는 ISO QKD 보안 표준, 안전한 데이터 전송의 새로운 시대를 열 것임

- ISO 웹사이트에 따르면, 기존 네트워크 구성 요소, 양자 광학 구성 요소 및 QKD 프로토콜의 전체 구현을 포함하여 QKD 모듈의 다양한 측면을 다루는 기본 **공통 보안 기능 요구 사항(common security functional requirements, SFRs) 세트를 설정**함

- SFR 분석이 용이하도록, QKD 모듈이 운영 환경에서 직면할 보안 문제에 대한 포괄적인 연구 수행, 이 분석은 QKD 모듈의 보안 기능에 대한 구조적 평가와 QKD 프로토콜 분류를 기반으로 함

- QKD 모듈 내 기존 네트워크 구성 요소와 관련된 SFR은 더 광범위한 ISO/IEC 15408 프레임워크 내에 통합됨, 암호화 모듈 및 네트워크 장치 테스트를 관리하는 관련 표준과 함께 ISO/IEC 19790에 설명된 방법론을 활용함

- 169개 국가 표준 기관의 회원국, 독립적 국제기구인 ISO는 전문가들을 모아 글로벌 과제를 해결하고 혁신을 장려하는 자발적인 합의 기반 국제 표준 수립

- QKD 보안 표준의 출시는 끊임없이 진화하는 디지털 위협 환경

속에서 강력한 사이버 보안 솔루션을 육성, 이러한 표준은 양자 통신 시스템의 보안을 보장하는 중추적 역할 수행, 보다 안전하고 탄력적인 디지털 미래의 중요 단계를 표시함

○ ISO 표준(ISO/IEC 23837)

- 정보 보안: 양자 키 분배(QKD)를 위한 보안 요구 사항, 테스트 및 평가 방법 규정, QKD 모듈의 SFR 명시
- 이론적으로 QKD는 사전 공유 키를 사용하여 상대의 계산 능력에 의존하지 않는 보안과 더 긴 대칭 키를 설정하는 방법을 제공함, 설정된 키는 암호화 목적(안전한 통신 채널 생성)으로 암호화 메커니즘에 사용될 수 있음
- QKD 프로토콜의 보안성은 사전에 두 통신 당사자가 비밀 키를 공유한다고 가정하는 엄격한 보안 모델을 통해 입증, QKD 모듈의 수명 주기 단계에서 모델과 실제 구현 간 불일치가 자주 발생
- 이러한 불완전성이나 보안 모델의 편차는 실제 QKD 시스템의 보안성을 손상시키는 취약점을 초래할 수 있음, 그중에서도 심각한 측면 채널 공격이 제안되었고, QKD 해킹 실험에서 몇 가지 원리 증명 시연이 있었음

(원문)

1. https://thequantuminsider.com/2023/08/30/iso-releases-standards-for-quantum-key-distribution-security/
2. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:23837:-1:ed-1:v1:en