세계 최초 양자 위성에서 보안 취약점 발견

(2025.06.04. 양자정보연구지원센터)

□ 세계 최초 양자 위성 '미커스(Micius)' 보안 취약점 분석 보고서

○ 중국이 발사한 세계 최초의 양자 통신 위성 Micius의 보안 취약점 발견(arXiv 게재)

- 위성 내부의 레이저 타이밍 불일치로 인해 암호 키가 외부 공격자에게 노추될 가능성 존재

○ **BB84 프로토콜의 구현 취약성**

- Micius는 BB84 프로토콜과 decoy-state 기법을 혼합하여 양자 키 분배(QKD)를 수행
- 이론상 보안이 보장된다고 알려진 BB84 방식이었으나, 하드웨어 결함으로 인해 실제 구현에서 보안 구멍 발생

○ **레이저 타이밍 불일치**

- 위성 내 8개의 레이저 다이오드 사용(신호용 4개, 디코이용 4개)
- 일부 레이저에서 **최대 300피코초의 시간 지연** 발생(예: 수직 편광 상태의 디코이 레이저 Vd가 신호보다 312ps 늦게 발사됨)
- 이는 광 펄스 길이(200ps)보다 긴 시간차로, 포톤 도착 시간에 **명확한 지문(Fingerprint)**을 남김

○ 부채널(Side channel) 공격 가능성

- 공격자는 시간 지연 데이터를 통해 신호/디코이 구분 가능
- 시뮬레이션 결과: 신호/디코이 상태를 98.7%의 정확도로 구분 가능
- 이로 인해 암호 키 생성률이 0에 수렴, 암호화 완전 붕괴 가능성

○ 실험 및 데이터 근거

- 데이터 출처: 러시아 Zvenigorod 지상국과 Micius 간 양자 통신 실험(2021.10 ~ 2022.3)

- 분석 방식: 각 레이저 다이오드 별 포톤 도착 시점 비교를 통해 시간 지연 분석
- 대표 사례: 2021년 10월 31일, Vd 레이저가 대응 신호 레이저보다 312ps 늦게 동작

ㅇ 구조적 문제와 해결 불가성

- (**소프트웨어 수정으로 해결 불가**) 문제의 원인은 위성 설계 단계에서의 하드웨어 아키텍쳐 결정
- 다중 레이저 방식의 구조 자체가 시간, 스펙트럼, 방향성 등에서 차이를 유발할 수 있음
- Micius는 궤도상에서 레이저 타이밍을 조정할 수 있는 기능이 없어 **발사 이후 수정 불가능**
- (**동기화 주장에 대한 반론**) 초기 논문은 레이저가 10ps 이내로 동기화됐다고 주장
- 본 연구는 이 주장에 의문을 제기하며, **타이밍 검증의 방법론 또는 설계상의 시스템적 허점** 가능성을 지적

ㅇ 향후 양자 위성 시스템에 대한 시사점 및 연구 한계점

- (**이론적 보안은 실용적 보안과 다름**) BB84 및 양자 암호는 수학적으로는 안전하지만, 실제 장치의 물리적 결함은 보안 취약점으로 연결될 수 있음
- 특히 우주 환경에서 온도, 진동, 노후화 등의 외적 요인이 시스템 성능에 영향
- (미래를 위한 권고 사항) 단일 레이저 + 전기광학 변조기(EOM)를 활용한 시스템 아키텍쳐 고려, 발사 전 정**밀 하드웨어 동기화 테스트** 필수
- **얽힘 기반 QKD 시스템** 도입 검토

(원문)

1. https://thequantuminsider.com/2025/06/03/study-finds-security-flaw-in-worlds-first-quantum-satellite/