

# MadQCI 확장 가능한 양자 키 분배 네트워크로 보안통신 인프라 개선

(2024.09.26, 양자정보연구지원센터)

- MadQCI(Madrid Quantum Communications Infrastructure), 보안 통신 인프라 개선하는 확장 가능한 양자 키 분배 네트워크
  - 마드리드 공대 화웨이, Toshiba Europe 등 여러 유럽 기관 협력, 마드리드 양자 통신 인프라(MadQCI) 개발
    - MadQCI는 실제 환경에서 작동하는 확장 가능하고 이질적인 양자 키 분배(QKD) 네트워크
    - 양자 통신과 기존 통신 기술의 통합으로 양자 통신의 상용화 가능성 제시
  - MadQCI의 새로운 패러다임
    - (기존 QKD 네트워크 문제점) 기존 네트워크는 고정된 인프라로 구축되며, 확장성과 비용 효율성 문제 존재
    - 연구 환경에서는 효과적이거나 상용화에는 비효율적
    - (MadQCI의 해결책) 소프트웨어 정의 네트워킹(SDN) 패러다임 도입으로 네트워크 유연성 및 확장성 증대
    - 기존 통신 인프라와의 통합 가능성 향상, 비용 절감
  - 네트워크 구성
    - 28개의 QKD 모듈과 9개의 노드로 구성
    - 마드리드 광역 지역에 배치된 노드들이 광섬유를 통해 연결
    - 양자 통신과 기존 통신이 같은 물리적 인프라에서 공존, 상업적 실현 가능성 높임
    - 상용 통신 인프라를 활용해 비용 효율적 운영 가능
  - 네트워크의 유연성과 통합
    - (MadQCI의 동적, 모듈형 아키텍처) 기존 QKD 네트워크는 어두운 광섬유(dark fiber)를 사용하여 제한적인 연결만 가능

- MadQCI는 광 스위치와 SDN 컨트롤러를 사용하여 필요에 따라 양자 링크를 동적으로 설정
  - 네트워크 내 직접 양자 연결의 수를 늘리고, 확장성과 복원력 향상
  - (상호운용성 강화) 다양한 QKD 기술과 프로토콜을 지원하는 아키텍처로 다양한 장치 및 벤더 간 상호 운용성 제공
  - 네트워크 운영자는 새로운 장치나 기술을 쉽게 통합 가능
- 실제 응용 사례
- (3년간 네트워크 테스트 및 개선) 여러 구간에서 오랜 기간 동안 중단 없이 안정적 운영
  - 다양한 부문에서 안전한 통신 제공, 실생활에서 요구 사항 해결
  - (MadQCI의 주요 활용 사례)
  - **중요 인프라 보호:** 100명의 사용자를 위한 4Gbps 암호화 데이터 전송
  - **안전한 네트워크 관리:** 24초만에 소프트웨어 이미지 배포, 자가 복구 기능 제공
  - **클라우드 서비스:** QKD 서비스로 초당 1,230개 보안 키 생성 요청 처리
  - **5G 사용 사례:** 초저지연(0.15ms)으로 5G 보안 통신 지원
  - **e-헬스 서비스:** 실시간 및 비실시간 헬스케어 통신 암호화 (500Mbps, 지연 1.3ms)
  - **순차 데이터 전송 증명(Ordered Proof of Transit, OpoT):** QKD 기반 데이터 패킷 보안 태깅으로 패킷 당 5.86ms 지연 추가
- MadQCI는 미래 양자 통신 인프라의 청사진
- 유럽 양자 통신 네트워크 구축 위한 EuroQCI 프로젝트에 기여 가능성
  - MadQCI 운영에서 얻은 교훈이 차세대 양자 네트워크 개발에 기여
  - 양자 안전 통신 기술의 광범위한 채택을 촉진

(원문)

1. <https://thequantuminsider.com/2024/09/04/madqci-a-scalable-quantum-key-distribution-on-network-improving-secure-communications-infrastructure/>