양자암호통신 기반의 국가바이오빅데이터 보안 인프라 구축 연구

이원혁
한국과학기술정보연구원
livezone@kisti.re.kr

A Study on building national bio-big data security infrastructure based on quantum cryptography communication

Wonhyuk Lee
Korea Institute of Science & Technology Information

요 약

국가 차원의 바이오빅데이터는 정밀의료, 유전체 연구, 전염병 대응 등 다양한 분야에서 핵심적 자산으로 활용되고 있다. 본 연구에서는 국가바이오빅데이터를 운영하는 센터 간 중요 데이터를 양자암호통신(Quantum Key Distribution, QKD) 기반의 안전한 네트워크로 구축하는 방안을 제시한다. 기존 암호화 방식의 보안 취약성을 극복하고, 포스트 양자 시대에 대비한 데이터 보안 인프라로서 QKD의 도입은 국가 생명정보 보호의 핵심 전략으로 간주된다. 본 논문에서는 국가 중요 바이오데이터의 전송에서 양자암호통신망 기반의 전용망을 구축한 사례를 통하여, 관련 기술 개요, 시스템 아키텍처, 운영 시나리오, 보안성 효과에 대해 고찰한다.

Ⅰ. 서 론

4차 산업혁명의 도래와 함께 보건의료 분야는 데이터 중심의 정밀의료(precision medicine)로 급속히 전환되고 있다. 유전체 정보, 임상 기록, 생활습관 등 다양한 개인 건강 정보를 통합·분석함으로써 질병을 예측하고, 조기 진단 및 맞춤형 치료를 실현하려는 노력이 지속되고 있다. 이를 가능하게 하기 위해서는 고품질의 바이오헬스 데이터를 안정적으로 확보하고, 이러한 민감한 정보를 안전하게 전송·공유할 수 있는 보안 인프라가 필수적이다. 이에 따라 국가 연구과제로 추진중인 '국가 바이오빅데이터 구축 사업'을 통해 정밀의료 및 바이오헬스 산업의 경쟁력을 강화하기 위한 기반을 마련하고 있다.

본 사업은 보건복지부와 과학기술정보통신부 주도로 2020년부터 시작되었으며, 유전체, 임상, 생활습관 정보를 통합한 100만 명 규모의 바이오빅데이터를 구축하는 것을 목표로 한다. 특히, 이와 같이 수집된 고민감성 데이터를 안전하게 전송·저장하기 위하여 보다 안전한 전송 및 공유 체계를 구현하고자, 한국과학기술정보연구원(KISTI)과 국립의과학지식센터 간에 양자암호통신 기반의 보안 네트워크가 구축되어, 의료 데이터를 물리적으로 보호할 수 있는 인프라를 구현하였다. 이는 양자컴퓨터 시대의 위협에도 견딜 수 있는 차세대 보안 기술로서, 향후 중요 민감 데이터의 전송 및 공유 체계에 중요 참조가 될 것이다.

최근 관련 연구로서, 양자암호 기술을 활용하여 헬스케어 데이터의 암호화를 보다 효율적으로 강인하게 수행하는 방법을 연구하거나, 무인 항공기를 이용한 농업 모니터링 시스템에서 양자키분배 시스템을 통하여 데이터 보안을 강화하는 방안을 연구하기도 하였다[1],[2].

또한 양자컴퓨팅 시대를 대비하여 생명과학 및 헬스케어 시스템의 보안 회복력을 확보하기 위한 포스트양자 암호기술의 로드맵을 제시하거나, QKD 시스템의 최신 보안 취약성과 이에 대한 기술을 종합적으로 분석한 관련 대응 연구도 수행되고 있다[3],[4]. 또한 정부 및 의료 부문의 장기적 통신 보안을 보장하기 위해 양자키분배의 실제 적용 사례와 기술적 전망을 제시하고 분석하는 연구도 수행되고 있다[5],[6].

본 논문에서는 KISTI-국립의과학지식센터 간 양자암호통신망 구축 사례를 중심으로 바이오헬스 데이터의 보안성 확보 방안을 고찰한다. 또한 양자암호통신망 구축, 연계 모델로서 제시하고자 한다.

Ⅱ. 본론

양자암호통신은 양자역학 원리에 기반하여 비밀키를 절대적으로 안전하게 분배할 수 있는 기술이다. QKD는 키 생성 과정에서 도청 여부를 탐지할 수 있으며, 도청 시 키 교환이 실패함으로써 정보 유출을 원천적으로 차단할 수 있다. 정부는 디지털 뉴딜 정책의 일환으로 초연결·초안전 사회 구현을 목표로 하여, 이 양자보안기술을 국가 핵심 인프라에 적용하기 위한 양자암호통신 인프라 구축 사업을 추진한 바가 있으며, 주요 공공기관 및 연구기관 간에 양자암호 기반 네트워크 설치한 국가적 검증을 수행한 바 있다.

빅데이터 공유환경을 위하여 오픈환경에서 컨트롤 엑세스의 최고치 보안 네트워크 환경을 구축하기 위하여, 양자암호 기술 중 양자키 분배 기술(QKD:Quantum Key Distribution)을 통해 송수신단이 대칭키를 안전하게 나누어 갖으며, 이를 통해 기존 광통신에서 고려되지 않는 물리계층의 보안을 확보하였다. 기존 암호체계는 양자컴퓨터 등의 출현으로 해킹 가능한 위험에 노출되어 있으며, 광통신에서 물리계층의 보안은 고려되지 않아, 전송 네트워크의 중간지점에서의 정보 탈취에 취약성을 가진다.

바이오 빅데이터 센터 간 QKD 기반 통신망 아키텍처 구성을 위하여 각

바이오빅데이터 센터에 양자키 분배 장치를 설치하여 키 생성을 수행하기 위한 QKD 장비와 기존 광통신망에 양자채널(QC 채널)과 고전채널(CC 채널)을 병행 구축하고, 생성된 키를 암호화 시스템에 연동하고, 만료 및 교환 정책을 관리하는 키 관리 시스템(KMS)을 통하여, QKD 기반으로 생성된 키를 이용해 바이오 데이터를 고속 암호화/복호화 수행하는 암호화 응용 계층을 서비스하는 구조로 이루어져 있다.

폐쇄망을 구성하는 전용회선은 타 네트워크와 물리적으로 분리되는 단독회선을 기준으로 원본데이터 저장시스템, 분석시스템만을 직접 연결하여 대형 데이터의 전송, 백업, 저장을 위한 송수신 기능을 제공하며, 유전체 데이터 생산기관의 1G-10G급 데이터전송망은 보안전송망과 동일한 구조의 전송구조 확장을 통해 구축된다. 보안전송망은 원본데이터 공유와 백업을 위한 100G급 전용망, 허가된 접근에 해당되는 사용자(기관) 및 자원간 접속망, 유전체 데이터 생산기관간 보안전송망 구축을 순차적으로 구축·진행한다.

바이오데이터는 대용량 파일로 전송되므로, QKD로 생성한 키를 통해 대칭키를 암호화하고, 이후 해당 대칭키를 통해 데이터를 암호화하는 방식으로 운용된다. 이를 통해 실시간 고속 전송과 양자 수준의 보안성을 동시에 확보할 수 있다. 도청이나 키 유출 시 시스템은 즉각 키 분배를 중단하고, 새로운 키를 재생성한다.

보안성 측면에서 QKD 기반 통신은 기존 RSA, ECC 기반 통신과 달리 수학적 난제에 의존하지 않으며, 양자컴퓨터의 연산 성능에 관계없이 보안을 유지할 수 있다. 물론, 국가 과학기술연구망(KREONET)을 기반으로 전용망을 구성하고, 각 기관의 양단간에는 각종 보안장비를 통하여 계층별 암호화 및 보안 대응 체계를 구축하고 있다. 특히나 전송구간에서는 양자암호통신을 통하여 각 기관간의 구간 암호화에 양자역학적 성질을 이용한 안전성을 구현하였다.

이렇게 구성된 보안 전송망을 통한 고속환경과 오픈환경에서의 컨트롤 엑세스의 안전한 환경에서 안정적으로 운영하기 위하여, 바이오빅데이터 고속전송을 위해 구축된 보안전송망은 사업참여기관과 사업단내 대규모 데이터 전송을 위한 폐쇄망과 접속허가를 획득한 연구자(기관)이 접근 가능한 2개의 계층으로 구성하여 운영한다.

사업 참여기관 중 대규모 데이터 전송이 필요한 기관 간 고속 전용 전송망을 구축하고, 연결된 네트워크는 타 네트워크와 물리적으로 접속이 차단된 상태로 강화된 보안과 대규모 유전체 데이터 전송성능이 유지되는 완전 오픈& 컨트롤 엑세스의 최상위 보안망 구축을 기본으로 추진한다. 연결된 네트워크는 데이터 사업단 참여 기관에 위치한 스토리지 데이터의 전송 전용망으로 구축되어 외부기관에서 사용하는 트래픽과 충돌 방지와 고정된 대역폭으로 공유되는 데이터 전송 성능 최고치를 목표로 추진하며, 바이오빅데이터의 접근에 허가받은 연구자 누구나 접근 가능한 서비스망 운영을 위해 방화벽 중심의 오픈&컨트롤(open & controlled) 엑세스 구축 운영한다.

오픈&컨트롤(open & controlled) 엑세스 구축 시 네트워크 속도(대역폭)는 각 연동기관의 데이터 보유량, 공유될 데이터 및 실시간 송수신 크기, 백업 등을 중심으로 계산되어 할당될 것이며, 오픈&컨트롤(open & controlled) 엑세스는 물리적 또는 논리적으로 연동되어 목적에 따라 접근 권한을 차등하여 운영하며, 완전 폐쇄망부터 허락받은 연구자 누구나 접근이 가능한 서비스망까지 포함한다.

Ⅲ. 결론

국가 바이오빅데이터 구축 사업과 양자암호통신 국가 사업은 각각 정밀의료와 데이터 보안이라는 분야에서 국가 미래 전략기술을 대표할 수 있으며, 의료데이터 기반 정밀의료 혁신과 차세대 보안 인프라 구축의 시너지를 창출할 수 있다. 특히, 유전체 및 임상 정보와 같은 민감정보인 바이오 데이터를 안전하게 수집·전송·분석하기 위해 양자암호통신망(QKD)을 도입함으로써, 정밀의료의 실현 기반이 되는 데이터의 기밀성과 무결성을 확보할 수 있다. 향후에는 KISTI-국립의과학지식센터 간의 양자통신망과 같은 시범 사례를 전국 바이오데이터 허브 및 의료기관으로 확대하고, 이를 통해 의료기관 간의 실시간 보안 데이터 연계, AI 기반 맞춤치료 플랫폼과의 연동, 그리고 양자보안 기반 클라우드 의료 서비스 등으로 확장함으로써 국가적 차원의 의료·보안 융합 인프라를 구축해 나갈 것으로 기대한다.

ACKNOWLEDGMENT

이 논문은 2025년도 한국과학기술정보연구원(KISTI)의 수탁과제 “바이오빅데이터 플랫폼 구축 및 운영(N24NT056-25, RS-2024-00438573)”으로 수행된 연구입니다.

참 고 문 헌

[1] Basha, C. B., Murugan, K., Suresh, T., SrirengaNachiyar, V., Athimoolam, S., & Pappa, C. K, Enhancing healthcare data security using quantum cryptography for efficient and robust encryption, Journal of Electrical Systems, 2024

[2] Karagodsky, V., & Kassab, M, Application of quantum key distribution to enhance data security in agrotechnical monitoring systems using UAVs. Applied Sciences, 15(5), Article 2429, 2024

[3] Sahi, A., & Nayyar, A, Post-quantum healthcare: A roadmap for cybersecurity resilience in biomedical systems. Journal of Biomedical Informatics, 142, 104391, 2023

[4] Kim, Y. J., & Lee, H, Quantum cryptography for securing personal health information in neonatal care. Journal of Newborn Biology, 8(3), 112 - 117, 2023

[5] Huang, P., Zeng, J., & Liu, Y., Quantum key distribution: A survey on current vulnerability trends, Optics Continuum, 3(8), 1438 - 1455, 2022

[6] Zeilinger, A., Ursin, R., & Boaron, A., Long-term secure government and medical communications with QKD, Toshiba Quantum Technology Reports, 2021

[7] Sharma, R., & Kaur, P., Quantum cryptography in healthcare information systems, Journal of Emerging Technologies and Innovative Research, 9(8), 145 - 152, 2022

[8] Patel, D., & Shukla, H., Quantum key distribution networks: Key management – A survey. arXiv preprint. arXiv:2408.04580, 2024