

양자통신 테스트베드 동향

Trends in Quantum Communication Testbeds

김인규 (I. Kim, kig547@etri.re.kr)

양자기술연구본부 책임연구원

주정진 (J. Ju, jjju@etri.re.kr)

양자기술연구본부 책임연구원

ABSTRACT

With the advancement of quantum computers and increasing importance of cybersecurity, quantum cryptography has become an essential technology in quantum world. The success of ground-to-satellite quantum communication in the range of 4,600 km has been reported, and intercountry quantum cryptography connecting the UK and Ireland has been demonstrated. In the European Union, OpenQKD has established 18 testbeds for quantum communication in 12 countries. Through the progress from experimental to pilot networks, quantum cryptography testbeds have begun to provide networks for commercial services, such as finance, healthcare, and government administration. Similarly, the Republic of Korea launched a quantum communication testbed project to accelerate the development of quantum communication devices and materials. The project also aims to support the relevant companies and services in the verification and certification of security functionalities operated by the National Intelligence Service. We review the status of quantum communication testbeds in 16 countries.

KEYWORDS 양자(암호)통신, 양자내성암호, 양자인터넷, 양자키분배, 양자통신테스트베드, 위성양자통신

1. 서론

양자암호(Quantum Cryptography)[1]와 양자 키 분배(QKD: Quantum Key Distribution)[2] 기술의 개발과 더불어 광섬유를 통하거나 자유공간에서 적은 수의 광자를 이용한 양자통신이 시작되었다[3,4]. QKD에서는 양자역학을 이용해서 도청 여부를 감시한다. 즉, 양자적 특성을 이용해서 비밀키를 안전하

게 분배하는 것이 핵심이며, 단일광자를 이용하는 BB84 프로토콜과[2,5] 얽힘 광자를 이용하는 E91 프로토콜[6-8] 등이 활용된다. 양자통신은 실현 가능성을 증명하는 단계를 넘어서 캠퍼스와 캠퍼스, 도시와 도시, 국가와 국가, 그리고 지상과 우주를 연결하는 형태로 발전하고 있으며, 여러 국가에서 상용망 서비스가 시작되고 있다[9,10]. 양자컴퓨팅 기술과 함께 양자 정보를 처리하고 교환할 수 있는

* DOI: <https://doi.org/10.22648/ETRI.2024.J.390509>

* 본 보고서는 과학기술정보통신부와 한국지능정보사회진흥원(NIA)의 지원을 받은 “양자기술 시험검증 및 컨설팅 지원 한국전자통신연구원” 사업과 과학기술정보통신부 지원을 받은 “양자인터넷 구현을 위한 유선 양자중계기 개발(2022-0-00463)” 사업의 일환으로 작성함.



양자인터넷[11] 개발이 궁극적인 목표로서, 양자정보를 저장하는 양자 메모리[12-15]와 네트워크 노드 사이에서 양자 정보를 연결하여 원거리 통신이 가능하게 해주는 양자 증계기(Quantum Repeater)[16-20] 등에 대한 많은 연구가 진행되고 있다.

양자통신과 양자인터넷에 사용되는 소·부·장 품목으로는 앞에 언급한 양자메모리 외에도 양자암호 발생기(QRNG: Quantum Random Number Generator), 단일광자 검출기(SPD: Single Photon Detector), 결맞음 광 검출기(Coherent Photodetector), 양자광원(Quantum Source), 양자간섭계(Quantum Interferometer), 양자키분배(QKD) 장치, 양자키관리 시스템(QKMS: Quantum Key Management System), 양자암호화기(QENC: Quantum Encryptor) 등의 부품과 장치들이 막대한 시장을 형성하면서 발전 중이다. 양자통신의 핵심 기술인 QKD 기술 상용화 업체로는 표 1에 보인 것처럼

IDQ, TOSHIBA, KETS, QNu Labs, Quintessence Labs, KEEQUANT, ThinkQuantum, HEQA Security 등이 있으며, 수 km에서 100km 이상 거리에 대해 서비스를 제공하고 있다[21].

불과 10여 년 전까지만 해도 각 나라에서 양자정보과학의 비전을 제시하면서 정부 차원의 투자와 인력양성을 시작하였는데[9], 이제는 관련 부품과 장비뿐만 아니라 양자통신망을 상용화 수준으로 서비스하는 수준에 도달하고 있다. 이렇게 빠르게 발전하는 양자통신 시장에서 양자통신 부품과 장비들을 실제 양자통신이 이루어지는 환경에서 테스트하고 성능을 고도화할 수 있도록 지원하는 양자통신 테스트베드의 기술적 수준도 빠른 속도로 고도화되어 가는 추세이며, 점차 테스트베드와 상용망이 공존하는 형태가 늘어나고 있는 것으로 보인다. 양자통신 테스트베드는 기술 개발의 단계에 따라서 실험망(기술개발 및 시연), 시험망(장거리 시연 및 네트워크

표 1 QKD 기술을 공급하는 세계의 기업들

회사명	국가	제품명	거리	프로토콜	키 생성 속도
IDQ	스위스/한국	Clavis XG	150km	BB84	14,000 AES-256 keys/hour
		Cerberis	90km	COW	
		Clavis 300	70km	한국표준 LEA, Galois counter mode	6kbps / 10kbps
TOSHIBA	일본 (재 영국 quantum lab)	Multiplexed System	70km	BB84	40kbps
		Long Distance System	120km	BB84	300kbps
KETS	영국	Chip-base	-	-	-
QNu Labs	인도	Armos	40~60km	distributed phase reference	128kbps(40km) 1~2kbps(60km)
Quintessence	호주	qOptica 100	5~40km	CV-QKD	240kbps(5km) 4.3kbps(40km)
KEEQUANT	독일	PIC-base	-	CV-QKD	-
ThinkQuantum	이탈리아	-	100km	BB84 (DV)	2.2kbps 13dB
HEQA Security	이스라엘	Loqomo1	-	BB84	-

출처 "Quantum communication market 2024-2034: Technology, trends, players, forecasts," IDTechEX, 2024. 1.도표의 저작권은 IDTechEX에 있으며, IDTechEX의 동의하에 사용되었습니다. 추후 이용 시 IDTechEX에 문의하시기 바랍니다.

크 안정성 시험), 시범망(응용 서비스 실증), 그리고 상용망(상용서비스 제공)으로 구분할 수 있는데, 2019년 기준으로 유선양자암호(QKD) 분야에서 미국과 중국은 상용서비스망까지 구축하고 있고, 유선양자전송 분야에서는 미국과 이탈리아가 시험망을, 그리고 무선양자전송은 중국, 싱가포르, 유럽에서 실험망을 구축하고 있으며, 위성양자전송은 중국과 오스트리아가 실험망을, 일본이 시험망까지 구축한 것으로 보고된 바 있다[9]. Global Quantum Intelligence 사는 전 세계 걸쳐서 구축되어 있거나, 해체된, 그리고 설립이 발표된 상태의 양자네트워크 테스트베드를 망라한 44개의 리스트를 게시한 바 있다[22]. 대부분의 양자통신 네트워크는 한 나라 내에서 도시와 도시를 연결하거나 도시 내의 주요 거점을 연결하는 형태로 구축되어 있으며, 지상과 위성을 연결하기도 하고, 영국과 아일랜드를 해저 광섬유로 연결한 경우처럼 국가와 국가를 연결하는 양자통신 네트워크가 구축되고 있기도 하다. 다수의 나라가 인접하고 있는 유럽에서는 OpenQKD 프로젝트를 중심으로 각국의 양자통신 네트워크를 연결하여 국가 간 양자통신 네트워크, 더 나아가 양자통신 인터넷을 구축하려는 연구도 진행 중이다. 본고에서는 북미, 유럽, 아프리카, 아시아 지역에 걸친 각 지역의 대표적인 양자통신 테스트베드 동향에 대해 기술하였다.

II. 북미지역 양자통신 네트워크

1. 미국

뉴욕, 일리노이, 워싱턴DC, 캘리포니아, 메릴랜드 등에 다수의 양자통신 테스트베드가 존재하며 주로 대학과 국립연구소 중심으로 구축되어 운영되고 있다.

가. 뉴욕

1) LIQR

롱 아일랜드 지역의 광섬유망에 구축된 테스트베드로서 Brookhaven National Laboratory(BNL), Stony Brook University(SBU), 뉴욕시에 위치한 다목적 양자 노드(Quantum Nodes), Commack, Westbury, Garden City에 위치한 스와핑 노드(Swapping Nodes)로 이루어진 길이 약 356km 링 형태를 이루고 있으며, Long Island Quantum Ring(LIQR)이라고 부른다[23]. 이 테스트베드에서는 2019년 18km의 얽힘 광자 전송, 2020년 상용망을 통한 양자통신 큐비트의 140km 전송 기록을 달성한 바 있고, 2021년에는 양자메모리 운영을 추가하였다. SBU는 2022년 롱아일랜드 투자펀드로부터 지원을 받아 BNL과 함께 the Long Island Quantum Internet Test Bed를 구축함으로써 양자인터넷 기술의 글로벌 허브로 발돋움하고 있으며, 2024년에는 독립적인 상온 양자메모리에 단일 광자 수준의 펄스를 저장하는 결과를 발표하기도 하였다[24,25].

2) GothamQ Network

2023년, Qunnect[26]사와 NYU는 Brooklyn Navy Yard와 맨해튼의 NYS 캠퍼스를 잇는 16km 표준 광섬유를 통해 양자정보를 전송하는 데 성공하였고, 이 실험은 Qunnect 사의 양자네트워크인 브루클린과 퀸즈에 걸쳐서 구축된 상용 광섬유망을 이용하는 GothamQ에서 이루어졌다. 2024년에는 이 네트워크에서 편광기반의 얽힘 광자를 생성 및 분배하여 34km 광섬유 루프상에 보존할 수 있었다[27].

나. 일리노이

1) CQE+Toshiba

2022년에 시카고는 2020년에 구축된 144km 길이의 Argonne National Laboratory 양자 루프에 추가

로 56km 길이를 늘려서 총 200km 길이의 양자 네트워크를 구축하였고, CQE(Chicago Quantum Exchange) 과학자들을 주축으로 도시바와 함께 양자 보안 실험을 시작하였고, 이 시카고 네트워크는 학계와 산업계에 오픈하여 양자보안기술을 개발하는 테스트베드로 활용되는 미국 내 최초의 공공 테스트베드 중 하나로 운영된다[28].

2) AQNET-SD

2023년에 Fermi National Accelerator Laboratory (Fermilab)는 Advanced Quantum Networks for Scientific Discovery(AQNET-SD) 프로젝트를 위해 DOE로부터 900만 달러의 편당을 받고, 국가 규모의 양자 네트워크 구축에 나섰다. 페르미랩(Fermilab, FNAL)과 DOE Argonne National Laboratory(ANAL) 사이에 양자 네트워크를 구축하고 최적화하기 위해 양자-인코딩된 광자를 이용한 기술과 프로토콜을 개발한다. 또한 하이브리드 무선-유선 네트워크를 구축하며, 미래의 양자컴퓨팅 기술을 접목함으로써 양자통신과 양자컴퓨팅 기술을 향상시키는 데 기여한다. AQNET-SD는 뒤에 설명할 페르미랩이 이끄는 IEQNET(the Illinois-Express Quantum Network)의 성공에 기반하여 구축되고, 아르곤 내셔널 랩, 학계, 산업계 파트너를 포함한다. 이 양자 네트워크는 페르미랩, 아르곤랩, 스타라이트(Starlight)에 있는 시카고랜드 양자 노드 일부와 어바나 샴페인에 있는 일리노이대학의 양자노드를 포함하고, Kankakee, Rantoul을 경유한다. 하이브리드 무선-유선 양자 링크는 Caltech와 Jet Propulsion Laboratory(JPL) 사이에 구축된다[29].

3) IEQNET과 FQNET

IEQNET는 페르미랩의 주도하에 광대한 시카고 도시지역에 광 양자 네트워크로 구축되어 중계

기 없는 네트워크 기술을 개발하게 된다. 여기에는 페르미랩과 아르곤랩, Northwestern(NU)대학과 칼텍, 그리고 NuCrypt, HyperLight 같은 기업과 IEQNET AT&T/Caltech 컨소시엄이 참여한다. IEQNET 네트워크는 기존의 Fermilab Quantum Network(FQNET) 노드, NU대학 캠퍼스 노드, 그리고 ANAL 노드를 포함한다[30].

4) HQAN

Hybrid Quantum Architectures and Networks (HQAN)는 양자 프로세서와 네트워크의 하이브리드 결합을 통해 분산형 양자프로세싱을 통해 대형 양자컴퓨터를 구현하는 것을 목표로 NSF QLCI (Quantum Leap Challenge Institute)에서 추진한다. HQAN에 필요한 기술을 개발하기 위한 세 개의 테스트베드는 (1) 분산 프로세서와 네트워크 테스트베드, (2) 분산 정보처리, 네트워크 프로토콜, 소프트웨어 개발, (3) 보호된 큐비트(Protected Qubits)로 구성된다[31].

다. 워싱턴 D.C.

1) DC-QNet

DC-QNet은 2022년에 체계가 만들어졌으며, 실생활 영역의 양자 네트워크 테스트베드를 구축하기 위한 6개의 DC 지역연방기구 컨소시엄으로 구성된다. 6개의 기구는 Naval Research Laboratory(NRL), Army Research Laboratory(ARL), National Institute of Standards and Technology(NIST), Laboratory for Telecommunication Sciences(LTS), US Naval Observatory(USNO), National Aeronautics and Space Administration(NASA)이다.

DC-QNet에서는 고 충실도 양자메모리 노드, 단일-광자 소자, 큐비트 플랫폼, 주파수 변환, 동기화 등의 기술 개발, 6개의 도시권 기구를 연결하는 네트

워크 인프라 개발, 노드들 사이에 양자 얽힘 전송 연구 개발, 네트워크 시뮬레이션, 교육, 소프트웨어 개발 등을 다룬다[32].

라. 메릴랜드

1) QuaNeCQT

Quantum Networks to Connect Quantum Technology(QuaNeCQT) 프로젝트는 NSF에서 500만 달러를 지원받아 Edo Waks(PI, UMD), Norbert Linke(co-PI, UMD), TriptiSinha(co-PI, UMD/MAX), Dirk Englund(co-PI, MIT), SaikatGuha(co-PI, U. Arizona) 등이 참여하여 진행한다. 이 프로젝트는 양자컴퓨터가 인터넷상에서 정보를 교환할 수 있는 기술과 하드웨어를 개발하는 것을 목표로 한다.

처음으로 개발하는 품목은 qFC(quantum Frequency Conversion) 모듈과 qROADM(quantum Re-configurable Optical Add-Drop Multiplexer)로서 qFC는 양자 모델 기능을 수행하여 양자컴퓨터와 광섬유 네트워크의 인터페이스를 가능하게 하며, qROADM은 양자 라우터로서 양자 원격전송을 이용해 양자 결맞음 상태를 유지하면서 신호를 전송할 수 있도록 해준다. 개발되면 이온-트랩 양자컴퓨터와 단일광자 검출기를 포함하는 연구실 사이를 연결하는 MARQI(the Mid-Atlantic Region Quantum Internet) 네트워크에 배치하게 되며, 참여자로는 IonQ, 메릴랜드대학의 새로운 양자컴퓨팅 이용자 테스트베드인 Q-bed 등으로 확장될 예정이다[33].

2. 캐나다

캐나다에서는 2016년에 캘거리대학(U. of Calgary)에서 17km 거리의 양자통신 실험망을 구축한 바 있으며, 그 이후에 추가적인 양자통신 테스트베드에 대해 보고가 없다가 최근 들어 양자통신 테스트베

드 구축을 위한 투자와 위성을 이용한 양자통신 프로젝트 등이 보고되고 있다.

가. 퀘벡주 양자통신 테스트베드

1) 양자통신 테스트베드 2.0

Numana 양자통신 테스트베드는 다음 두 가지 목적으로 구축된다. 즉, (1) 양자 네트워킹 기술과 첨단 양자 소자의 프로토타입 실증, (2) 양자 네트워킹 기술을 실험하고 실제 활용에 수용 전략을 가속화할 수 있도록 업체, 연구기관 등에 상용기술 개발 환경을 제공한다. Numana의 테스트베드는 광섬유 링크, 각종 장비를 갖춘 실험공간, 기본적인 QKD 구성블록, 그리고 필드 테스트에 필요한 사용자 요구 사항을 충족할 수 있는 다양한 네트워크 토폴로지 등으로 구성되고, 양자내성암호(PQC) 프로토콜과 QKD 프로토콜, 그리고 고전 유-무선 네트워크를 통합할 수 있도록 설계한다.

가까운 미래에 테스트베드 광섬유 링크상에 얽힘 분배를 적용하는 것도 계획되어 있다. 퀘벡주 정부의 펀딩으로 시작해서, 첫 번째 테스트베드를 Sherbrooke 시에 3노드 구성으로 구축, 두 번째 테스트베드 허브는 2023년 말에 몬트리올에 구축, 그리고 2024년 초에는 퀘벡주에 세 번째 테스트베드를 구축하는 로드맵을 수립해서 진행한 바 있다[34,35]. 2024년 6월에는 도시바와 전략적 제휴를 맺고 퀘벡 주의 양자테스트베드를 확장해서 2개의 노드를 추가하는 작업을 진행 중이다[36].

2) QEYSSat

Quantum Encryption and Science Satellite(QEYSSat)는 Canadian Space Agency(ASC/CSA) 펀딩으로 2025년에 발사할 계획이며, 지상-우주 통신을 위한 학습 양자 링크와 QKD에 기술 데모 플랫폼 제공한다. QEYSSat은 저궤도 위성으로서 지상의 관제소와

양자 인코딩된 광자를 교환할 수 있는 양자 송수신기를 갖출 예정이다[37].

III. 유럽의 양자통신 테스트베드

유럽은 EU의 지원을 통해서 많은 나라가 양자정보기술을 활발하게 연구 개발하고 있는 곳이다. 2004년 유럽 위원회(Europe Commission)의 프로젝트로 11개 EU 국가와 러시아, 스위스의 41개 연구그룹과 산업 파트너가 참여하여, QKD 네트워크의 보안, 설계, 통신프로토콜 개발과 테스트베드 운영 등의 목표를 수행한 바 있는 SECOQC[3], 유럽 전역 12개국 18개 테스트베드를 운영하고, 노키아, 도시바, IDQ 등 38개 파트너와 함께 48개의 유즈케이스를 시험, 실증하는 OpenQKD[38], 네덜란드, 독일 등 유럽 7개국 주도로 10년 내 유럽에 양자암호통신망을 구축하는 프로젝트로 2019년에 출범한 EuroQCI(European Quantum Communication Infrastructure)[39] 등 다양한 프로그램을 통해 유럽 각국에서 독자적인, 혹은 컨소시엄을 통한 양자통신 테스트베드를 구축하고 있다. 이들과 연계된 몇몇 국가의 양자통신 테스트베드 구축 상황을 살펴본다.

1. 룩셈부르크

2022년 룩셈부르크대학교가 국무부와 협력해서 양자통신 인프라 연구소인 LUQCIA 설립을 발표하였고, EU 펀딩을 받아 5년 프로젝트를 통해서 국가 테스트베드를 구축하고, 양자키분배와 양자 인터넷 분야의 첨단 응용 연구를 꾀한다[40].

2. 네덜란드

네덜란드는 2023년에 유럽위원회 공동 펀딩으로

QCINed를 출범하고, 네덜란드에 유즈케이스 개발과 시험을 위한 양자시스템과 양자네트워크 환경 구축, EU에서 개발되고 제작되는 소자, 기술, 시스템을 사용함으로써 유럽의 기술적 자립에 기여 등의 미션을 수행한다. QDK 네트워크는 Utrecht 지역, Amsterdam-the Hague 지역, Eindhoven 지역의 세 곳에 구축되고, 지역마다 각각 거점 네 곳을 연결하며, the Hague-Aslmeer 구간에 정부 데이터 교환을 위해 정부 부처들 간의 연결망을 구축하고 하고 있다[41,42].

3. 이탈리아, 슬로베니아, 크로아티아

EuroQCI 프로젝트의 일환으로 유럽의 세 나라인 이탈리아, 슬로베니아, 크로아티아를 광섬유 양자네트워크로 연결하여 Inter-Europe 양자네트워크를 구축하였고, 타임-빈 인코딩과 BB84 프로토콜을 사용하였고, 두 개의 송신단(Alice)과 세 개의 수신단(Bob)으로 구성하여, 각각 서비스 신호와 양자 신호를 전달하는 두 개의 광섬유 연결을 구축하였다. 이탈리아 Trieste-슬로베니아 Postojna에서 2kbps, 슬로베니아 Ljubljana-Postojna에서 3.1kbps의 키 생성률을 기록하였고, 고 손실(25dB) 구간인 Trieste-크로아티아 Rijeka에서는 610bps를 기록하였다. 분배된 양자키를 이용하여 사용자 간의 VPN(Virtual Private Network)의 보안을 강화하였고, 2021년 Trieste에서 개최된 G20 행사에서 양자-보안 비디오-콜에 적용하였다[43].

4. QIA와 Open QKD

가. QIA

Quantum Internet Alliance(QIA)의 미션은 필요한 하드웨어와 소프트웨어 서브시스템의 개발, 집적

화, 그리고 성능시연을 통해 범-유럽 얽힘 기반 양자인터넷을 위한 청사진을 개발하는 것이다. 기술적으로 다음의 내용을 포함한다. 즉, 3, 4개의 원격 양자 네트워크 노드 간 얽힘과 원격전송, 양자메모리 기반 양자 중계기 기술 개발로 장거리 링크를 구현한다. QIA는 유럽연합 Horizon 2020 펀딩을 받아서 운영된다[44].

나. Open QKD

2019년에서 2023년에 걸쳐서 1,800만 유로 규모의 QKD 테스트베드 인프라 구축 프로젝트로 12개국 18개의 테스트베드를 구축하였고, 35개 이상의 QKD 시스템을 포함한다. 헬스케어, 에너지, 금융, 정부, 모빌리티 내비게이션, 연구, 교육, 데이터센터, 클라우드, 스토리지, 컴퓨팅 등 다양한 유즈케이스를 다룬다[38,45].

5. 영국

가. UKQN

영국 캠브리지와 브리스톨을 연결하는 광섬유 기반의 총 연장 410km 길이의 영국 최초의 양자네트워크인 UKQN(UK Quantum Network), 그리고, 캠브리지와 Suffolk BT Labs 사이의 세계 최초 상용급 양자 테스트 네트워크 링크 UKQNtel 등의 양자통신 테스트베드가 구축되어 있다. UKQN은 National Dark Fibre Facility를 활용하는 R&D를 위한 네트워크로서, 4개의 링크와 3개의 중간 노드를 갖는다[46].

나. UKQNtel

UKQNtel은 2019년부터 운영되기 시작했고, 기존의 표준 상용 광섬유망을 활용해서 125km의 길이에 걸쳐서 구축되어 있다. 이 네트워크는 양자-

보안(Quantum-Safe) 통신 기술을 위한 테스트베드를 제공한다[47].

6. 영국과 아일랜드

2023년에 영국 Portrane과 아일랜드 Southport 사이를 224km의 광섬유로 연결하여 Rockabill Subsea Network를 구축하여 국가 간 최초의 양자통신을 구현하였으며, 해저구간을 포함한다[48]. 이 프로젝트는 York대학교와 Quantum Communications Hub, 그리고 euNetworks Fiber UK Ltd.(euNetworks)가 참여하여 구축하였고, euNetworks 사의 해저케이블을 사용하였다.

7. 러시아

러시아는 2021년에 National Research Technological University “MISIS” (NUST MISIS)와 the Moscow Technical University of Communications and Informatics(MTUCI) 캠퍼스를 연결하는 대학 간 양자네트워크를 최초로 발족하였다. 이는 러시아에서 양자암호를 이용해서 데이터를 보호하는 기술기반의 해법을 적용한 첫 사례이다. 이 네트워크는 NUST MISIS와 MTUCI 건물에 위치한 5개의 노드로 구성되지만, 새로운 참가자가 등장하면 스케일-업할 수 있는 열린 구조를 갖는다[49].

8. 남아프리카공화국

아프리카 지역에는 2008년에 남아프리카 공화국의 더반시에 양자통신 테스트베드가 구축되었고, 이로 인해 더반시는 세계 최초의 QuantumCity가 되었다. eThekweni Municipality 광통신 인프라상에 양자통신 보안 솔루션을 구현한 것으로, 4개의 노드

MAN 스타 네트워크 구조를 가지고 있으며 연결거리는 1.5km에서 30km 사이에서 가변적이다[50].

IV. 아시아의 양자통신 테스트베드

아시아 지역에서는 일본, 중국, 인도, 싱가포르, 그리고 우리나라의 양자통신 테스트베드에 관하여 다룬다.

1. 일본

가. 도쿄 QKD 네트워크(QKDN)

2010년에 NICT에서 제공하는 오픈 테스트베드 광섬유 네트워크 JGN-X 상에 구축하였고, 신뢰노드들을 통해 QKD 링크가 연결된다. 4개의 기업 NEC, Toshiba, MELCO, NTT와 8개의 대학, 그리고 2개의 국가 연구소가 참여하였다[51]. 도쿄 QKDN은 최근 들어 다음과 같은 로드맵으로 발전해가고 있다[52].

- 1단계(~'23): 관동 지역 양자보안 클라우드 배치
- 2단계(~'25): 각 도시 양자보안 클라우드 배치
- 3단계(~'30): 위성-지상 네트워크 결합(일본 전역)
- 4단계(~'35): 글로벌 네트워킹

2. 싱가포르

가. NQSN

2022년에 싱가포르 Quantum Engineering Programme(QEP)은 세 개의 국가 차원의 양자기술 플랫폼을 출범시켰는데, 그중에 국가 양자 보안 네트워크(NQSN: National Quantum-Safe Network)가 포함된다. NQSN은 2022~2025년의 초기 단계에 양자 물리 법칙으로 보장하고 보호되는 양자-보안 통신 플랫폼을 설계, 구현, 운영하고 유지하는 목표를 수행

하고, 정부 기관과 사설 업체에 상용 기술을 보급하여 시험을 이어갈 예정이다. 또한 PQC(Post-Quantum Cryptography)도 함께 탐색하여 양자컴퓨터 해킹 대비 암호 알고리즘 탑재를 위한 소프트웨어 개발도 수행한다[53,54].

나. NQSN+

2023년에는 싱가포르 최초로 전국적인 규모의 양자 보안 네트워크(Quantum-Safe Network)인 National Quantum-Safe Network Plus(NQSN+)를 구축할 기업으로 SPTel(SP Engineering과 SP Group, 그리고 Spectral의 합동 벤처)사를 지정하기도 하였다[55].

3. 인도

2023년에 인도의 첫 번째 양자컴퓨팅 기반 통신망을 사용할 수 있게 되었음이 발표되었으며, 이 통신망은 Sanchar Bhawan과 뉴델리 CGO Complex에 있는 National Informatics Centre 사무실을 연결한다[56].

4. 중국

중국은 2018년에 상용 백본망상의 Zhucheng과 Huanshan 구간 66km에 QKD를 구현하여 키 생성률 ~5kbps를 보고한 이후[57], 2021년에는 Hefei USTC 연구팀에서 700개 이상의 지상 광섬유와 두 개의 지상-위성 연결을 통해 4,600km 거리에서 QKD 성공을 발표하기도 하였다. 이에 앞서 2016년 세계 최초로 양자통신용 위성(QUESS, Mozi/Micius)을 지구 궤도에 올려서 2,600km 떨어진 지상의 관제소와 QKD를 성공한 바 있고, 2017년에는 베이징과 상하이 사이 2,000km 길이의 광섬유망에서 QKD를 성공한 바 있다. 위성-지상 QKD에서 키 생

성률은 47.8kbps까지 달성하고 있다. 또한, 활용면에서 신뢰 릴레이를 이용해서 지상 QKD망과 지상-위성 QKD 망을 통합하여 중국 내 150개 기업 이용자에게 서비스를 제공할 수 있는 환경을 구축하고 있다. 사용자 그룹에는 은행, 전력망, e-정부 웹 등이 포함된다. 중국은 국제적인 파트너인 오스트리아, 이탈리아, 러시아, 캐나다 등에까지 네트워크를 확장할 계획을 가지고 있으며, 중궤도, 원궤도 위성을 이용하여 10,000km 대의 QKD 달성을 목표로 하고 있다[58].

5. 한국

2016년에 SKT가 분당-용인 구간 양자암호통신 시험망 구축하였고, 2018년에는 KOREN을 활용하여 SKT QKD와 국제 전송장비와 연동하여 서울-판교 간 양자암호통신기술을 적용하였으며, 2019년에 성수-둔산 간 5G 상용망에 양자암호기술 적용하였다[59]. 2022년에는 SK브로드밴드(SKB)에서 국가융합망 각 구간을 약 30여 개의 양자중계기로 연결하여 총 800km에 달하는 전국망 규모의 양자암호망을 구축하는 데 성공하였고, 48개 정부 부처 통신망을 하나로 연결하여 양자암호통신을 적용할 수 있게 되었다. 2023년에는 국내 최초로 QKD와 양자내성암호(PQC) 모두 지원하는 전용회선 서비스를 출시하였다[60].

2024년에는 한국지능정보사회진흥원 주관으로 개방형 양자 테스트베드를 구축하고 운영하는 사업을 시작하여, 한국과학기술연구원(KIST), 한국정보통신기술협회(TTA), 한국전자통신연구원(ETRI), 한국표준과학연구원(KRISS)의 4개의 거점 기관에서 시험과 검증을 제공하고 있다[61-63]. 이에 더해 4개 거점을 연결하는 양방향 양자암호통신망 및 양자인터넷 실증환경을 제공, PQC 시험검증 인프

라 구축 등을 위해 약 200km 거리의 판교-대전, 약 50km 거리의 서울-판교, 50km 내외의 판교 거점 양자테스트베드를 구축한다.

V. 결론

QKD를 이용한 양자통신 테스트베드는 상용화 서비스가 가능한 수준까지 발전하였고, 구현 가능한 거리도 지상에서 2,000km까지 도달하고 있고, 영국과 아일랜드의 구축 사례와 같이 국가와 국가를 연결하는 장거리 양자암호통신기술이 구현되고 있다. 얽힘광원을 이용한 양자통신은 아직 전송거리가 짧고 신뢰성 있는 키 생성률이 낮아서 실용성은 부족하지만 양자물리학의 얽힘 특성을 그대로 반영하는 미래 기술로서 실현되었을 때 그 파급효과가 매우 클 것으로 기대된다.

양자통신 테스트베드는 양자암호통신기술 개발을 위한 목적에서 한 걸음 더 나아가 양자프로세서 등 기기 간 연결을 양자적으로 제공하는 양자인터넷으로 발전해 나가는 추세이다. 미국 QuaNeCQT가 그런 예를 보여주는 대표적인 양자통신 테스트베드라고 할 수 있다.

우리나라는 세계적인 수준의 광통신기술을 기반으로 비교적 짧은 시간에 유무선 QKD 기술 분야에서 실용화 단계까지 발전하고 있고, SKT, SKB, KT, LGU+ 등 통신사에서 양자통신 상용망을 구축하고 있으며, 전국에 걸쳐 정부 기관 등에 서비스를 제공하고 있다. 특히 QKD와 PQC를 결합한 양자통신 서비스를 세계 최초로 선보이는 등 선도적인 역할을 수행하고 있다.

앞으로는 전 국토 규모의 양자통신 망을 구축하고, 더 나아가 양자인터넷 시대를 여는 데 필수적인 양자중계기, 양자메모리 개발 등에 인력과 자본의 투자가 필요하다고 생각된다. 또한, 글로벌 양자통

신의 실용화에 매우 중요한 기술로 평가되고 있는 지상-위성 양자통신은 세계 최고 기술을 보고하고 있는 중국에 비해 10년에 가까운 기술 격차가 있어서 정부출연연구소, 학계, 기업 등의 관심과 적극적인 투자가 절실한 분야이다.

용어해설

양자키 분배(QKD) 양자물리의 고유한 특성을 이용해서 통신자간에 비밀키를 공유하는 기술

양자통신 테스트베드 양자통신기술 개발 업체, 연구자들이 소재·부품·장비의 성능, 안정성, 상호호환성 등을 검증하는 인프라

약어 정리

ANAL	Argonne National Laboratory
AQNET-SD	Advanced Quantum Networks for Scientific Discovery
ARL	Army Research Laboratory
ASC/CSA	Canadian Space Agency
BNL	Brookhaven National Laboratory
CQE	Chicago Quantum Exchange
CV QKD	Continuous-Variable QKD
EuroQCI	European Quantum Communication Infrastructure
Fermilab FNAL	Fermi National Accelerator Laboratory
FQNET	Fermilab Quantum Network
HQAN	Hybrid Quantum Architectures and Networks
IEQNET	Illinois-Express Quantum Network
JPL	Jet Propulsion Laboratory
LIQR	Long Island Quantum Ring
LTS	Laboratory for Telecommunication Science
MARQI	Mid-Atlantic Region Quantum Internet
MTUCI	Moscow Technical University of Communications and Informatics
NASA	National Aeronautics and Space Administration

NIST	National Institute of Standards and Technology
NQSN	National Quantum-Safe Network
NRL	Naval Research Laboratory
NUST MISIS	National Research Technological University
PQC	Post-Quantum Cryptography
QENC	Quantum Encryptor
QEP	Quantum Engineering Programme
QEYSSat	Quantum EncRYption and Science Satellite
qFC	quantum Frequency Conversion
QIA	Quantum Internet Alliance
QKD	quantum Key Distribution
QKMS	quantum Key Management System
QLCI	Quantum Leap Challenge Institute
QRNG	Quantum Random Number Generator
qROADM	quantum Re-configurable Optical Add-Drop Multiplexer
QuaNeCQT	Quantum Networks to Connect Quantum Technology
SBU	Stony Brook University
SKB	SK Broadband
SPD	Single Photon Detector
UKQN	UK Quantum Network
USNO	US Naval Observatory
VPN	Virtual Private Network

참고문헌

- [1] S. Wiesner, "Conjugate coding," SIGACT News, vol. 15, no. 1, 1983, pp. 78-88.
- [2] C.H. Bennet and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," In Proc. IEEE Int. Conf. Comput., Syst., Signal Process., (Bangalore, India), 1984, pp. 175-179.
- [3] 과학기술정보통신부, 한국지능사회진흥원, 미래양자융합포럼, "2023 양자정보기술백서," 2023.
- [4] 윤천주 외, "무선 양자암호통신 시스템 및 부품 최신 기술 동향," 전자통신동향분석, 제33권 제6호, 2018, pp. 94-106.
- [5] H-L. Yin et al., "Tight security bounds for decoy-state quantum key distribution," Scientific Reports, vol. 10,

- 2020, 14312.
- [6] A. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, 1991, pp. 661-663.
- [7] A. Ling et al., "Experimental E91 quantum key distribution," in *Proc. of SPIE*, vol. 6903, 2008, 69030U-1-69030U-5.
- [8] 로드니 반 미터 지음, 남기환 옮김, "양자 인터넷, 양자 네트워크 기술의 이론과 실제," 에이콘출판, 2023, pp. 161-167.
- [9] 박성수, 송호영, "양자정보통신기술 현황과 전망," *전자통신동향 분석*, 제34권 제2호, 2019, pp. 60-72.
- [10] 한국경제신문, "SKT,美서 세계 두 번째 양자암호통신 상용망 구축," 2020. 1. 19.
- [11] S. Wehner et al., "Quantum internet: A vision for the road ahead," *Sci*, vol. 362, 2018, p. 6412.
- [12] P. Wang et al., "Single ion qubit with estimated coherence time exceeding one hour," *Nature Commun.*, vol. 12, 2021, p. 233.
- [13] C.M. Knaut et al., "Entanglement of nanophotonic quantum memory nodes in a telecom network," *Nature*, vol. 629, 2024, pp. 573-578.
- [14] S. Lieu et al., "Candidate for a passively protected quantum memory in two dimensions," *Phys. Rev. Lett.*, vol. 133, no. 030601, 2024.
- [15] Y. Zhou et al., "Long-lived quantum memory enabling atom-photon entanglement over 101km of telecom fiber," *PRX Quantum*, vol. 5, no. 020307, 2024.
- [16] Q-C. Sun et al., "Entanglement swapping over 100 km optical fiber with independent entangled photon-pair sources," *Optica*, vol. 4, no. 10, 2017, pp. 1214-1218.
- [17] S. Wengerowsky et al., "Entanglement distribution over a 96-km-long submarine optical fiber," in *Proc. Natl. Acad. Sci. USA*, vol. 116, no. 14, 2019, pp. 6684-6688.
- [18] J. Yin et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, 2020, pp. 501-505.
- [19] D. Niu et al., "All-photon one-way quantum repeaters with measurement-based error correction," *npj Quantum Inform.*, vol. 9, no. 106, 2023.
- [20] K. Azuma et al., "Quantum repeaters: From quantum networks to the quantum internet," *Rev. Mod. Phys.*, vol. 95, no. 045006, 2023.
- [21] T. Skyrme, "Quantum communication market 2024-2034: Technology, trends, players, forecasts," *IDTechEX*, 2024, pp. 16-17.
- [22] <https://quantumcomputingreport.com/where-are-the-worldwide-quantum-networking-testbeds/>
- [23] <https://www.bnl.gov/instrumentation/quantum/research.php>
- [24] S. Gera et al., "Hong-Ou-Mandel interference of single-photon-level pulses stored in independent room-temperature quantum memories," *npj Quantum Inform.*, vol. 10, 2024, 10.
- [25] <https://www.rfsuny.org/rf-news/sbu-quantum-internet/sbu-quantum-internet.html>
- [26] <https://www.qconnect.inc/>
- [27] <https://thequantuminsider.com/2024/04/19/qconnect-team-generates-distributes-preserves-entangled-photons-over-34-kilometers-of-gothamq-network-fiber/>
- [28] <https://news.uchicago.edu/story/chicago-quantum-network-argonne-pritzker-molecular-engineering-toshiba>
- [29] <https://news.fnal.gov/2023/10/fermilab-receives-doe-funding-to-further-develop-nationwide-quantum-network/>
- [30] <https://ieqnet.fnal.gov/>
- [31] <https://hqan.illinois.edu/about>
- [32] <https://www.nist.gov/programs-projects/quantum-communications-and-networks>
- [33] <https://www.thequilt.net/quilt-circle-article/quanecqt-project-aims-to-connect-quantum-computers-to-a-quantum-internet/>
- [34] <https://www.insidequantumtechnology.com/news-archive/numana-quantum-communication-testbed-2-0-an-innovation-tool-for-all-players-in-the-ecosystem/>
- [35] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Barry_Sanders_Presentation.pdf
- [36] <https://news.toshiba.com/press-releases/press-release-details/2024/Strategic-Collaboration-Between-Toshiba-and-Numana-to-Strengthen-the-Capabilities-of-the-Kirq-Quantum-Communication-Testbed-in-Quebec/default.aspx>
- [37] <https://uwaterloo.ca/institute-for-quantum-computing/qeyssat>
- [38] 김영희 외, "양자암호통신 테스트베드 구축과 활용방안에 관한 연구," 2022년 한국통신학회 하계종합학술발표회, 0429.
- [39] <https://qt.eu/ecosystem/quantum-communication-infrastructure>
- [40] https://gouvernement.lu/en/actualites/toutes_actualites/communiqués/2022/04-avril/06-laboratoire-infrastructure-communication-quantique.html
- [41] <https://quantumdelta.nl/qcined>
- [42] 유형정, "양자기술: 양자컴퓨팅 및 양자암호통신 기술 동향과 산업 전망," *TTA저널* 제205호, 2023, pp. 55-62.
- [43] D. Ribezzo et al., "Deploying an Inter-European quantum network," *Adv. Quantum Technol.*, vol. 6, no.

- 2200061, 2023.
- [44] <https://qt.eu/projects/communication/qia>
- [45] https://epic-photonics.com/wp-content/uploads/2021/10/Andreas-Poppe_OpenQKD.pdf
- [46] <https://www.quantumcommshub.net/research-community/about-the-hub/phase-2/work-package-1/>
- [47] <https://newsroom.bt.com/testing-begins-on-uks-ultra-secure-quantum-network-link-ukqntel-between-research-and-industry/>
- [48] <https://www.businesswire.com/news/home/20231003629118/en/For-the-First-Time-Researchers-Successfully-Demonstrate-Over-euNetworks%E2%80%99-Fibre-Infrastructure-That-Quantum-Communication-Is-Possible-Between-the-United-Kingdom-and-Ireland/>
- [49] <https://thequantuminsider.com/2021/10/20/first-ecosystem-interuniversity-quantum-network-launched-in-russia/>
- [50] <https://quantum.ukzn.ac.za/quantumcity/>
- [51] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Masahiro_Takeoka%20_Presentation.pdf
- [52] <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2023/0724/Documents/Kenyoshi.pdf>
- [53] <https://www.quantumlab.org/about/highlight/2022-05-singapore-national-quantum-platforms>
- [54] <https://www.fraunhofer.sg/en/about/solutions/national-quantum-safe-network--nqsn-.html>
- [55] <https://finance.yahoo.com/news/sptel-speqtral-appointed-build-nqsn-031000343.html>
- [56] <https://quantumzeitgeist.com/india-achieves-major-milestone-with-operational-quantum-computing-based-telecom-network-link/>
- [57] Y. Mao et al., "Integrating quantum key distribution with classical communications in backbone fiber network," *Opt. Exp.*, vol. 26, no. 5, 2018, pp. 6010-6020.
- [58] <https://en.ustc.edu.cn/info/1007/3182.htm>
- [59] 김민형, "양자암호통신 테스트베드 및 표준화 동향," *AI Network Lab Insight*, vol. 5, 2019년 7월, NIA.
- [60] <https://blog.sk broadband.com/4636>
- [61] <https://www.etnews.com/20240513000298>
- [62] 김인규 외, "양자통신 소·부·장 OpenLAB 기술검증 및 양자통신검증센터," 제34회 통신정보 합동학술대회, 2024, S14-1.
- [63] 배인호, "양자 통신·센서 평가기술 센터 구축과 활용방안," 제34회 통신정보 합동학술대회, 2024, S14-2.