KISTI
ISSUE BRIEF

ISSN 2635-5728

과학기술인프라, 데이터로 세상을 바꾸다

https://doi.org/10.22810/2022KIB048

2022. 10. 24. 제48호

포스트 퀀텀 시대의 안전한 통신
- Quantum KREONET -

김용환 · 이원혁

최근 4차 산업혁명, 빅데이터 환경 등의 데이터 중심 연구환경이 강화되고 있으며, 100Gbps에 달하는 네트워크 전송용량은 물론, 5G를 통한 고성능의 유무선 네트워크가 구축, 확대되고 있다. 기존 컴퓨팅 파워의 증대와 연구데이터의 증가, 그리고 이를 연결하는 빠른 유무선 네트워크는 중요 연구환경에 대한 해킹 이슈를 제공하고 있다. 특히 양자 컴퓨터와 같은 새로운 컴퓨팅자원 및 알고리즘 등의 기술 출현으로 인하여, 보안 취약성이 더 높아져 국가별 양자컴퓨터 및 양자암호기술에 투자하는 비율이 점차 높아지고 있는 상황이다. 현재 상황에서는 양자키분배(QKD) 기술을 이용하여 안전한 양자암호통신망을 구축 서비스하기 위한 노력이 추진되고 있다. 양자키분배 프로토콜은 송수신자 사이의 통신을 보호하기 위하여, 기존의 공개키 방식이 아닌 새로운 기법으로 대칭키를 안전하게 분배할 수 있는 기법이다. 양자키분배 프로토콜은 양자역학적 특성을 사용하여 송수신자 사이에 합의된 암호키를 통신 채널을 통해 전달하는 것이 아닌, 임의의 비트열로부터 동일한 비트열을 추출할 수 있으며, 도청자의 유무를 감지할 수 있기 때문에 안전한 프로토콜이라 할 수 있다.

본 고에서는 이러한 양자키분배(QKD) 장비를 이용하여 안전한 통신네트워크를 구축하기 위한 국내외 활동과 KISTI에서 추진하고 있는 양자암호통신망 구축계획에 대하여 소개하고자 한다.

CONTENTS

1. 양자암호통신 개요

포스트 퀀텀시대의 보안

- **(양자컴퓨터)** 중첩과 같은 양자역학의 고유한 물리적 현상을 활용하는 양자비트 (Quantum bit) 기반의 확률적 연산 컴퓨터로, 구글은 2019년 53개의 양자비트 양자컴퓨터 칩을 발표함
- **(양자우월성)** 특정 문제에 대해 양자컴퓨터가 기존컴퓨터를 능가하는 연산성능이 증명된 경우, 해당문제에 대한 양자우월성이 달성되었다고 일컬음
- **(현재 보안기술에 대한 위협)** 현재 인터넷에서 사용하는 RSA 암호체계는 복잡한 계산을 요구하는 소인수분해와 같은 방법에 기반하며, 소인수분해 문제는 1996년 Peter Shor에 의해 양자우월성이 증명되었음
- **(포스트 퀀텀시대의 보안요구)** 따라서 도래하는 포스트 퀀텀시대에서의 안전한 통신을 위하여, 계산에 기반한 종래암호통신기술의 한계를 극복한 일회성패드 (one-time pad)와 같은 암호기술이 필수로 요구됨

양자암호통신이란

- **(양자암호통신)** 양자암호통신은 복제 불가성과 같은 양자의 내재적 특성을 활용한 통신의 물리적 보안기술이며, 특히 도래하는 포스트 퀀텀시대에서도 무조건적인 보안을 달성할 수 있는 기술로 기대되고 있음
- **(양자키분배)** 양자키분배(QKD)는 데이터암호화에 활용되는 양자키를 사용자 간 분배하고 관리하는 기술로써, 도청이 불가하다는 양자의 물리적 특성을 통해, 일회성패드를 현실적으로 구현할 수 있는 기술로 이해되고 있음

양자암호통신 국내외 현황

- **(국내외 시장현황)** 매우 높은 수준의 보안을 요구하는 정부부처, 국방, 금융, 통신사업자 등의 유무선 인프라 보호 및 인증을 위한 네트워크 보안시장 중심으로 형성되어 있음
- **(국내 시장규모)** 정보통신기술진흥센터에 따르면, 국내 양자암호통신관련 시장은 2021년 1,363억원 규모로 추산되며, 2025년엔 1조 4,051억원 선으로 성장할것이 전망됨
- **(세계 시장규모)** 세계 양자암호통신시장은 2020년 약 778백만 달러로 추산되며, 2030년에는 29,012백만 달러규모로 성장할 것이 전망되며 특히, 2030년에는 세계 전체 보안시장의 12% 규모 수준인 약 290억 달러 규모에 달할 것으로 전망됨

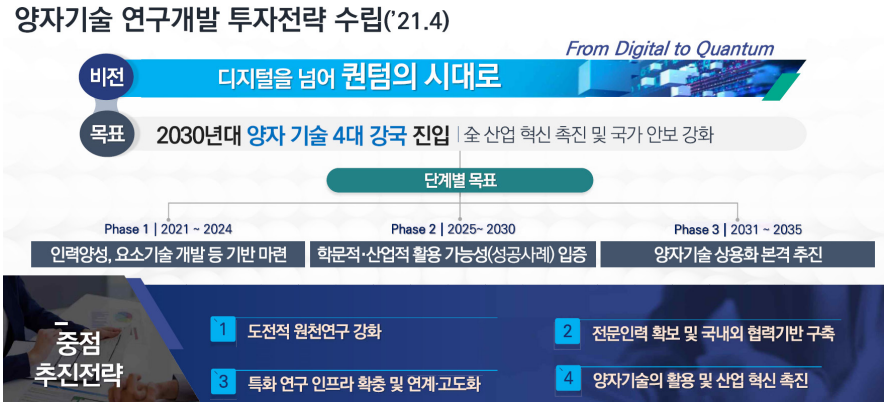
<그림 1> 양자암호통신 국내외 시장현황 및 전망

출처) 정보통신기술진흥센터 주간기술동향 & INI R&C 양자정보통신 최신동향 및 시장전망 보고서

• (국가정책기조)

- **(신정부 110대 국정과제)** "[75] 초격차 전략기술 육성으로 과학기술 G5 도약 (과기정통부)"에 따르면, (초연결 인프라) 전략기술·산업의 신속한 융합성장 촉진을 위한 5G·6G, 양자암호통신망, 위성항법시스템(KPS), 슈퍼컴 등 초연결 과학기술 인프라 구축을 목표로 함

<그림 2> 양자기술 연구개발 투자전략('21.12)



출처) 과학기술정보통신부 "양자기술 육성 방향 및 추진계획(안)" 발표자료

- **(양자기술 투자전략 수립)** 과학기술정보통신부는"디지털을 넘어 퀀텀의 시대로"라는 비전으로 2030년대 양자기술 4대 강국 진입을 위한 단계별 목표를 수립하고, ① 집약된 연구개발을 통해 핵심기술을 빠르게 추격, ② 시작단계에 있는 활용 분야 성과를 조기 창출하여 경쟁력 우위확보, ③ 국내외 협력 등을 통한 양자 핵심연구 인력 양성 및 확보, ④ 양자기술에 특화된 세계 최고 수준의 연구 인프라 확충, ⑤ 적극적 국제협력을 통한 기술 블록화에 선제 대응의 계획으로 추진

- **(관련 법률현황) 2020년 6월 정보통신융합법 개정에 따라 양자기술에 대한 정의, 기술개발, 인력양성, 클러스터 지정 등에 대한 국가지원의 근거가 마련됨**
  - **(양자정보통신 정의: 제2조의2)** 양자역학적 효과를 기반으로 하는 양자암호 및 통신, 양자센서 및 소자, 양자컴퓨터 등을 가능하게 하는 기술
  - **(진흥 근거: 제27조의2)** 연구개발지원, 인력양성, 인프라 구축, 시범사업, 표준화, 인증지원, 국제협력, 전달기관 지정 등에 대한 근거 마련 등
  - **(민간 지원: 제27조의3)** 민간분야 연구개발투자에 대한 지원 근거 마련
  - **(산업클러스터: 제27조의4)** 기업, 연구소, 대학 등을 상호연계하여 집중적으로 조성하기 위한 지역(양자산업 클러스터)의 지정근거 등 마련
- **(기술개발현황) 양자암호를 활용한 유선통신은 초기 상용화 단계이며, 무선통신은 장거리 기술 개발 중임**
  - **(중국)** 북경-상해 간 2,000km 양자암호통신 백본망을 구축 (2016) 하였으며, 드론을 이용한 무선양자얽힘 분배기술 (2020) 개발
  - **(미국)** 뉴욕 등 동부지역 양자암호통신 서비스 (2018)
  - **(영국)** ATM 용 초근거리 양자암호기술 개발 (2018)
  - **(대한민국)** KT, SKT 등 공공·산업·의료분야 시범망 구축 (2021)
- **(기술발전방향) 양자컴퓨터와 같은 다수의 양자기기를 연결하고 활용하는 양자인터넷 기술로 발전할 것으로 전망되며, 양자암호통신 기술은 도래하는 양자인터넷의 핵심기술로 기대됨**

2. 양자암호통신 핵심기술

양자키분배 기술

- **(개요) 양자키분배(Quantum Key Distribution, QKD) 기술은 빛의 양자적 특성을 이용하여 송수신자 간 대칭키를 분배하는 기술임**
  - QKD의 일반적인 수행 과정은 “양자상태 준비, 전송, 측정을 통한 키 시퀀스 생성 - 키 시프팅(sifting) - 도청 테스트 - 오류 정정과 비밀 증폭” 단계를 따름
  - 전송 채널이 자유공간(free space)인 경우를 무선 QKD, 광섬유(optical fiber)인 경우를 유선 QKD라 지칭함
  - QKD 프로토콜은 빛의 양자상태를 준비하고 측정하는 방식에 따라 구분할 수 있음

- **(불연속변수 QKD 프로토콜) 불연속변수(Discrete Variable, DV) QKD는 단일광자의 불연속적인 물리량을 이용한 상태 변조 및 측정을 기반으로 한 QKD 기술임**
  - **(BB84)** Charles Bennett과 Gilles Brassard가 1984년에 제안한 최초의 QKD 프로토콜로, 단일광자의 상태 변조와 측정을 기반으로 함. 송신자(Alice)가 서로 직교하지 않은 두 개의 기저를 구성하는 4개의 양자상태를 광자의 편광, 위상 등을 이용해 랜덤하게 변조 후 양자채널을 통해 전송하고, 수신자(Bob)는 두 기저 중 하나를 랜덤하게 선택하여 측정함으로써 원본 키 시퀀스를 생성함
  - **(Differential Phase Reference (DPR))** 약한 결맞음[1] 펄스 사이의 시간차 혹은 위상에 비트 정보를 기록하는 방식으로, BB84 프로토콜과 달리 랜덤한 기저 선택 과정이 필요하지 않으므로 시스템 구성이 상대적으로 간편함. 결맞음 펄스열의 진폭을 변조하는 프로토콜을 Coherent One Way(COW) 프로토콜, 위상을 변조하는 프로토콜을 Differential Phase Shift(DPS) 프로토콜이라고 함
  - **(E91)** 1991년에 Arther Ekert가 제안했으며, Alice와 Bob 양쪽이 얽힘광자쌍을 나누어 가진 뒤 각자 랜덤한 기저를 선택하여 측정을 수행함. 이 측정 결과를 이용하여 벨 부등식의 위반 여부를 결정함으로써 도청 여부를 파악할 수 있음
  - **(Measurement-device-independent(MDI))** 기존 QKD에서 보안에 가장 취약했던 부분인 측정부(검출기)에 대한 공격으로부터 보호할 수 있는 프로토콜로, 기존 프로토콜과 달리 Alice와 Bob 사이에 릴레이가 있는 구조임. Alice와 Bob이 BB84 프로토콜과 유사하게 편광 등을 랜덤하게 변조하여 독립된 양자 채널을 통해 릴레이로 전송하고, 릴레이에서는 수신된 광자들에 대한 벨 측정(Bell State Measurement)을 수행하여 그 결과를 공개 채널을 통해 공포함
  - **(Device-independent QKD)** DI-QKD 앞서 설명한 MDI-QKD가 측정장치에 대한 가정 없이도 수행할 수 있는 프로토콜이었다면, DI-QKD는 광원과 측정장치를 포함한 양자 장치들의 신뢰 여부에 영향을 받지 않는, 보안성이 한 단계 더 높은 프로토콜임

1) 빛의 결맞음 상태(coherent state)는 간섭성 상태라고도 하는데, 빛의 모드 수와 관계없이 1차 간섭성을 소유하고 있는 특성을 갖고 있음. 결맞음 상태의 빛은 이론적으로 1.2차 간섭성 및 모든 고차의 간섭성을 최대로 갖고 있는 빛의 특수한 상태를 가리키는데, 실제 레이저에서 방출되는 빛을 결맞음 상태를 이용하여 근사적으로 기술할 수 있음

- **(연속변수 QKD 프로토콜) 연속변수(continuous-variable) QKD는 결맞음 상태(coherent state)와 같은 특정 상태의 빛(전자기장)의 쿼드러처와 같은 연속적인 물리량의 변조 및 측정을 기반으로 한 QKD 기술임**
  - 변조 방식에 따라 가우시안 변조 결맞음 상태(GMCS, Gaussian Modulated coherent state), 불연속 변조 프로토콜로 나누어짐
  - 이론적 보안성 증명이 아직 점근적 한계(asymptotic limit)에서만 이루어져 있음
  - homodyne/heterodyne 검출 시스템과 같은 기존의 고전적인 코히어런트 광 검출기를 이용하여 측정이 가능하며, 통신 파장에서 단일광자검출기들과 비교했을 때 구축가격이 저렴한데도 불구하고 검출효율이 높음. 또한 기존 상용 광통신소자들과 호환성이 높아 다중화(multiplexing)를 통해 기존 광통신 인프라를 활용하기 유리함
  - 위상에 민감한 측정을 해야 하므로 위상 기준(phase reference)으로 사용되는 국부 진동자(local oscillator)의 잡음이 작고 위상 안정성이 높아야 하며, 전송 과정에서 광 손실의 영향을 많이 받으므로 100 km 이상의 장거리 통신에는 아직 적합하지 않음
  - 연속적인 측정값을 디지털 정보(키)로 변환해야 하므로 후처리 단계가 DV-QKD보다 복잡하여, 후처리 효율 개선에 대한 연구도 활발히 이루어지고 있음

양자키분배 네트워크 기술

- **(개요) 양자키분배 네트워크(Quantum Key Distribution Network, QKDN) 기술은 QKD 기반 네트워크를 구성하여 안전한 통신망을 구현하기 위한 것으로서, 신뢰하는 두 지점 사이에 양자기술을 이용하여 안전하게 비밀키를 분배하고, 이 비밀키를 활용하여 데이터를 암호화하여 교환하는 네트워크 기술임**
  - ETSI, ITU-T, TTA 등 다양한 국내외 표준에 따르면, 양자암호통신망은 QKD 계층과 양자키관리 계층, 그리고 서비스 계층으로 이루어지며, 국내외 표준화 기구에서 정의된 사항을 준수하여 구현함으로써, QKDN의 안전한 구현 및 활용이 가능함
- **(양자키관리시스템) 양자키관리시스템(Quantum Key Mangement System, QKMS)은 QKD로부터 양자키를 수신 및 관리하며, 양자암호 서비스 계층에 적절한 형태로 제공함으로써 양자암호통신망에서 양자키를 활용한 암호 서비스를 원활하게 제공하도록 함**
  - **(KMA, Key Management Agent)** QKMS-QKD와의 인터페이스를 위한 사우스바운드[2] API를 구현하며, QKD 장비로부터 양자키를 수신하여 저장, 동기화, 삭제 등 관리함

2) 네트워크를 구성하는 제어 평면과 데이터 전송 부분 간 연결

- **(KRA, Key Relay Agent)** QKMS 간 인터페이스를 위한 이스트-웨스트바운드[3] API를 구현하며, 중·장거리 및 다대다 QKD를 제공하기 위한 토폴로지 설정, 경로 설정 테이블 설정, 신뢰노드 기반 QKMS 간 양자키 전달 등을 수행함
- **(KSA, Key Supply Agent)** QKMS-서비스와의 인터페이스를 위한 노스바운드[4] API를 구현하며, QKD 응용서비스에 양자키를 서비스 보안 요구사항에 맞게 할당하고 관리함

• (기반 기술)

- **(SDN)** SDN(Software-Defined Networking)은 중앙집중형 방식의 SDN 컨트롤러를 기반으로 한 QKDN의 유연하고 프로그래밍 가능한 구성을 통하여 효율적인 네트워크 제어 및 관리를 수행함. 또한 SDN은 이기종 QKD 장비, QKMS, QKDN를 연계하여 통합하는 것을 단순화할 수 있는 방안을 제공함
- **(자원 할당)** 양자키 분배 네트워크를 운영하기 위해서는 양자 채널, 일반 채널, 데이터 채널을 모두 고려해야 함. 다양한 네트워크 채널의 효율적인 자원 할당을 위한 파장 분할 다중화(WDM, Wavelength Division Multiplexing), 시간 분할 다중화(TDM, Time Division Multiplexing), 공간 분할 다중화(SDM, Space Division Multiplexing) 방식이 존재함
- **(키 전달/라우팅)** QKD는 단대단 양자키 분배 기술이기 때문에 QKD 노드 사이에 직접적인 QKD 채널이 없을 경우, 네트워크 단위의 양자키 분배를 위해서는 임의의 두 노드 간의 양자키 전달이 요구됨. 한편, 네트워크 단위의 양자키 분배를 위한 QKMS이 별도로 존재하지 않는 경우 신뢰할 수 있는 양자암호통신 중계기(Trusted Repeater) 기반 양자키 분배 네트워크 구성 및 양자키 전달을 위한 라우팅 프로토콜이 요구됨
- **(키 풀링)** 일반적으로 단대단 QKD 시스템에서 달성 가능한 양자키 생성 속도는 QKD 프로토콜 및 거리에 따라 상이하겠지만 매우 낮기 때문에 충분한 양자키 암호화 서비스를 제공하기에 한계가 있음. 이에 따라, 희소한 양자키 자원을 효율적으로 활용하여 양자키 암호화 서비스의 연속성을 보장하기 위한 키 풀링(Key Pooling) 기술이 요구됨
- **(데이터 전송 경로 보호/복구)** 양자암호통신망을 구성하는 노드 및 채널 등의 물리적인 인프라에 장애가 발생하더라도 QKDN은 중단 없이 정상적으로 운영되어야 하며 제공 중인 서비스에 영향을 주지 않아야 함. 이와 관련하여 QKDN을 다중 경로로 구성하고 임의의 두 노드 간의 일반 경로 외에 보호 경로와 복구 경로를 선 지정하고 필요에 따라 선택하는 체계가 필요함
- **(비용 최적화)** 양자암호통신망을 구축하고 운영함에 있어 주요 진입 장벽 중 하나는 많은 비용이 소요되는 QKD 장비와 이들을 연결하는 다크 파이버임. 특히 QKD 백본 네트워크 구축은 규모가 크고 고려해야 할 사항이 다양하기 때문에 비용 최적화가 더욱 요구됨

3) 네트워크를 구성하는 제어 평면과 애플리케이션 간 연결
4) 네트워크를 구성하는 제어 평면 간 혹은 제어기 간 연결

3. 양자암호통신 구축동향

국내외 양자암호통신 구축동향

- **(개요) 양자암호통신은 양자키분배장비간에 안전하게 나누어진 키를 활용하여, 암복호화 등의 암호통신을 수행하는 형태로 구축됨**
  - 다양한 형태의 QKD 시스템을 기반으로 단대단 중심으로 구성가능하며, 다양한 프로토콜별로의 보안 안전성에 대한 수학적 증명 등은 전체적인 양자암호통신망의 안전성을 보장할 수 있는 중요한 요소임
  - 현재 DV-QKD 중심의 상용화 가능 QKD 장비는 거리의 한계로 인하여, 신뢰노드라고 칭하는 중간 중계기 형태로 구현하고 있으며, ETSI나 ITU-T 등의 표준화 문서에서 정의한 양자키 전달 표준에 맞춘 QKMS와의 접목을 통하여 구현되고 있음
- **(QKD 네트워크의 구현과 발전) 2002년 미 국방성 소속 DARPA(Defense Advanced Research Projects Agency)에 의해 최초의 QKD 네트워크가 구현된 이래, 2004년 EU의 SEOCQC(Secure Communication based on Quantum Cryptography), 2010년 일본의 도쿄 UQCC(Updating Quantum Cryptography and Communications), 2021년 중국의 대규모 QKD 네트워크 등이 구현된 바 있음**
  - **(미국, DARPA)** DARPA QKD 네트워크는 세계 최초의 양자키 분배 네트워크로 2002년 12월 공개됨. DARPA는 하버드 대학교와 보스턴 대학교 사이의 광 스위치를 통하여 구성되었으며 최대 거리 29km, 최대 양자키 생성 속도는 400bps임. DARPA는 QKD 시스템 간의 거리 한계를 극복하기 위하여 신뢰할 수 있는 양자암호통신 중계기와 스위칭 방식 모두 활용하여 양자키 분배 네트워크를 구축하였으며 양자키 리피터 프로토콜을 자체 개발하여 사용함
  - **(유럽, SEOCQC)** SEOCQC QKD 네트워크는 2004년에 유럽 위원회의 11개 유럽 연합 국가, 러시아, 스위스의 41개 연구 및 산업 파트너들이 참여한 FP6 프로젝트로 추진됨. SECOQC 프로젝트의 주요 목표는 QKD 네트워크 프로토콜의 보안, 설계 및 아키텍처, 통신 프로토콜, 구현, 데모 및 테스트 운영을 포함하여 QKD 네트워크 문제를 체계적으로 정리하는 것이었음. SECOQC는 신뢰할 수 있는 양자암호통신 중계기 기반 양자키 분배 네트워크를 구축하였으며, QKD 네트워크 통신에 대하여 저장 및 전달의 hop-by-hop 메시지 전송 방식을 채택함
  - **(일본, UQCC)** Tokyo UQCC QKD 네트워크는 2010년에 일본과 유럽 연합의 9개 기관이 참여한 NICT가 추진하는 Janpan giga Bit Network 2 Pluse 프로젝트 일환으로 추진된 테스트베드 네트워크. Tokyo UQCC는 SECOQC와 유사한 3-layer 구조를 사용하여 점대점 통신 백본망 형태로 구성하였으며, 기존 양자키 분배 네트워크는 달리 중앙 집중식 관리를 위하여 양자키 관리 서버를 처음으로 사용하여 양자키를 저장하고 망 운영 관리 데이터를 수집하였음

- **(중국, 대규모 QKD 네트워크)** 중국의 양자기술 연구그룹은 양자암호통신 분야 특히, QKD 네트워크를 대규모로 구현하는 연구 분야에서 독보적인 성과를 보이고 있으며, 2017년 위성을 릴레이로 활용한 최초의 대륙간 QKD 구현, 2021년 지상의 광섬유 기반 백본(backbone), 광역(metropolitan area) QKD 네트워크와 위성 QKD 릴레이 노드를 통합한 대규모 통합 네트워크 구현을 보고한 바 있음

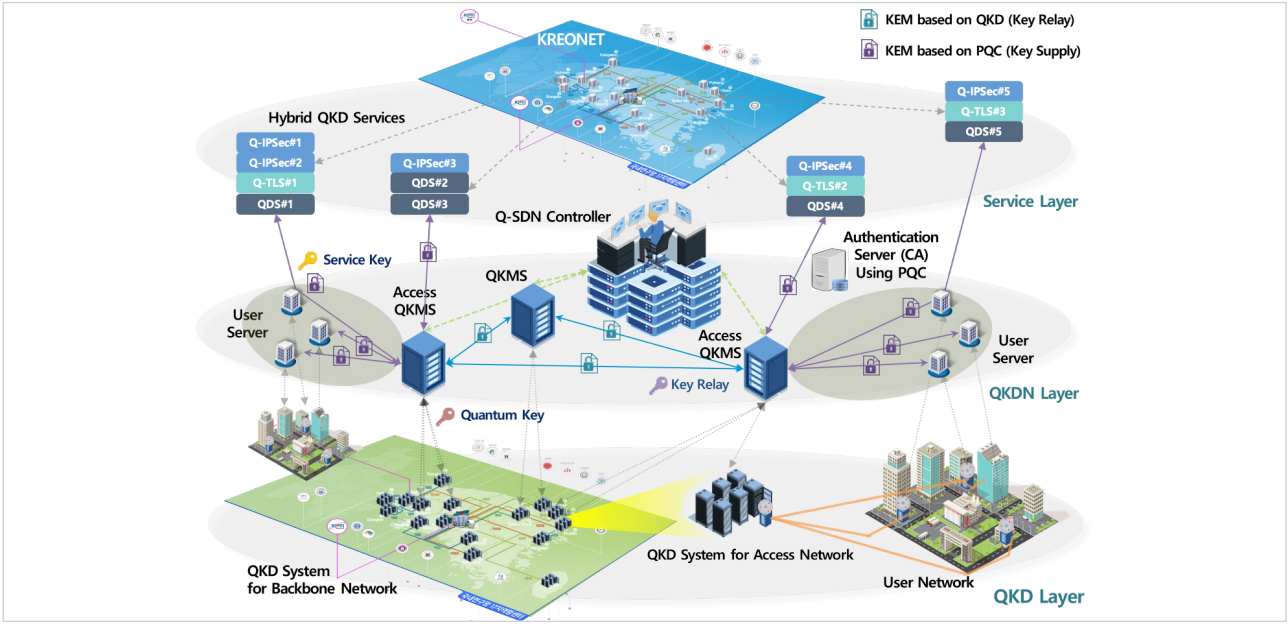
- **(국내 QKD 기술 동향)** SKT는 최장 거리 107km 링크를 포함하는 양자암호 네트워크 망을 구현, KIST와 KT는 공동연구를 통하여 서울 도심 내 5개 노드를 연결하는 QKD 네트워크를 구현한 바 있으며, KISTI는 QKD 프로토콜 구현 뿐 아니라 양자 암호키 관리 기술에도 투자하여, 최근 민간사와 양자암호통신망 표준 기반 양자키 관리 기술 이전 협약 체결을 보고한 바 있음

- **(기술 선도국 구현 계획)** 미국은 Long Island quantum network, IEQNET(Illinois Express Quantum Network) 등 양자 중계기 및 얽힘 분배 기술을 활용한 광역도시 규모 양자 네트워크를 구현 계획을 갖고 있으며, EU는 QIA를 통해 얽힘 분배 네트워크 구현 연구를 수행하는 동시에 EuroQCI(The European Quantum Communication Infrastructure) 계획을 통하여 얽힘 기반 양자키분배 구현을 고려하고 있음

- **(얽힘 기반 양자키분배)** 얽힘 분배를 활용할 경우 BB84 대비 높은 안전성을 보장할 수 있는 얽힘 기반 양자키 분배 프로토콜 구현이 가능하며, 특별히 얽힘 분배를 통해 부채널 공격(side channel attack)으로부터의 안전성을 보장하는 기기무관(device-independent) 양자키분배 구현이 가능하여, 이의 구현 기술 연구 추진

KISTI 양자암호통신 구축동향

<그림 3> KISTI 양자암호통신망 구조도

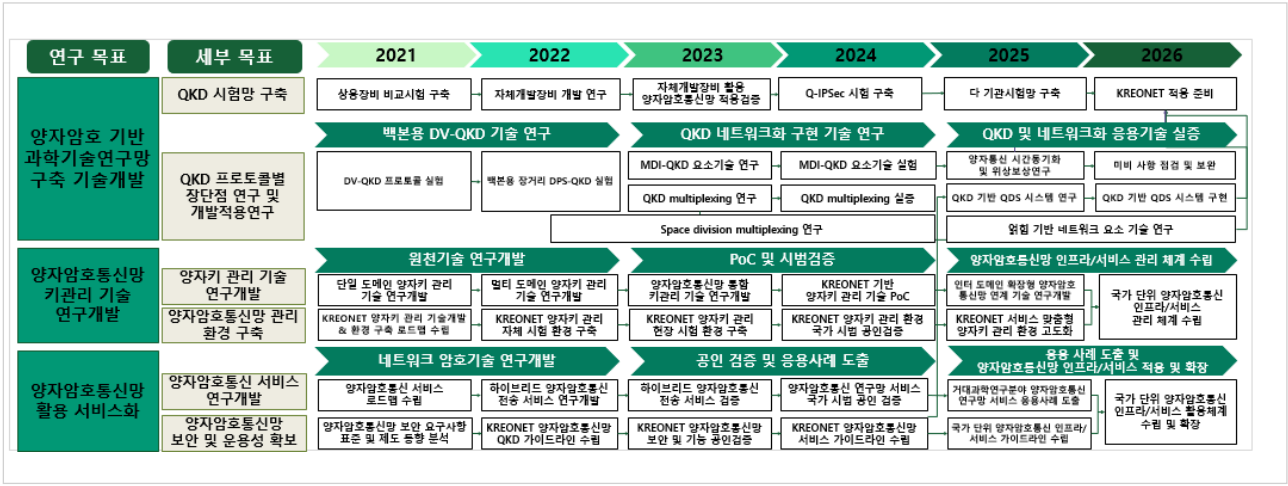


- **(KISTI QKD 기술 동향) KISTI는 KREONET과 같은 성형(Star Topology) 네트워크 구조에 적합한 Plug&Play 타입 BB84 QKD 장치를 제작하고, QKMS 및 IPSec 장치와 연동 시험함**
  - **(QKD 성능 안정화)** 온도, 습도 등의 환경변화에 의한 양자비트오류율(QBER) 모니터링 및 능동 시간지연 보정 기술을 적용하여 성능 안전화를 높임
  - **(테스트베드 환경 구축)** 국가 중요 연구데이터 센터간에 양자암호통신망의 테스트베드 환경을 구축하여, 상용 QKD 장비의 운영과 기능 사항을 분석하며, 안정적 양자암호통신망 구축 및 운영관리 소요 사항을 분석함
- **(KISTI QKDN 기술 동향) 국가 중요 연구데이터를 물리적 기반의 양자암호기술을 이용하여 안전하게 전송·공유할 수 있는 차세대 국가연구망 구축을 위한 QKDN 주요 기술 및 시스템을 개발함**
  - **(KREONET QKMS)** 양자키관리 계층 기반 중·장거리 QKD를 제공하고, 다양한 QKD 장비 및 암호 서비스들을 지원하며 KREONET 인프라 및 서비스 요구사항에 부합하는 KREONET QKMS를 표준을 준수하여 구축·개발함
  - **(KREONET Q-SDN-Controller)** 각 도메인마다 배치되는 QKMS들을 통합적으로 관리하며 멀티 도메인 양자키 전달 및 제어를 수행하기 위한 KREONET Q-SDN-Controller(양자키관리 환경 통합제어 컨트롤러)를 구축·개발함
  - **(표준 준용)** ETSI, ITU-T TTA 등 국내외 표준화 문서 기반으로 양자키를 End User간 전송할 수 있도록 QKDN 환경을 구축함
  - **(PQC 기술 연계)** KREONET 양자암호통신망 구축 시, KREONET이 관리하지 않는 유저 종단까지 QKD를 배치하는 일은 다양한 관리 및 정책상의 이슈를 야기하기 때문에 해당 네트워크 액세스 구간의 데이터 채널 암복호화와 인증에 양자내성암호(Post Quantum Cryptography, PQC) 기술을 연계·적용함
  - **(원천기술 확보)** 서비스 수준의 KREONET 양자암호통신망 운영·관리를 위한 다수의 QKDN 기반 기술을 자체 개발하여 보유하는 한편, 삼극특허를 포함한 다수의 국내외 지식재산권을 선점함

4. KREONET 양자암호통신 구축전략제언

사업 추진 로드맵

- KREONET은 전국 17개 지역망센터, 해외 4개 PoP으로 구성되어, 국가·공공기관 및 연구기관이 중요 연구데이터를 전송하고, 협력하고 있다. 광서킷망과 데이터 패킷망으로 구성되어 서비스하고 있으며, 양자채널을 구축하여 양자암호통신망 서비스를 제공하기 위해서는, 다양한 양자기술 요소와 서비스 방안이 고려되어야 한다. 이에 아래와 같이 국가과학데이터 전송을 위한 양자암호 인프라 전환방안을 수립하고, 서비스하기 위한 기술 확보를 추진하고자 한다.



- **(1단계) 양자암호통신망 필수 기술 개발 및 KREONET QKD/QKMS/양자암호서비스 개발**

  - 양자암호통신망 구축을 위한 QKD 상용장비 테스트와 QKD 프로토콜별 장단점 연구를 통한 연구망 적용 QKD 장비 개발 연구

  - 멀티도메인 양자키 관리 기술개발 및 연구망 적용을 위한 로드맵 수립을 통한 단계별 연구계획 수립

- **(2단계) 양자암호통신망 서비스화 기술 개발 및 KREONET QKD/QKMS/양자암호서비스 보안 및 기능 검증을 위한 국가공인검증**

  - 자체 개발된 DV-QKD를 활용한 양자암호통신망 실망 적용 검증 및 Q-IPSec연계를 통한 종단간 암복호화 기능 검증

  - QKD 프로토콜별 실험연구 및 네트워크화를 위한 다중화 기술연구 수행

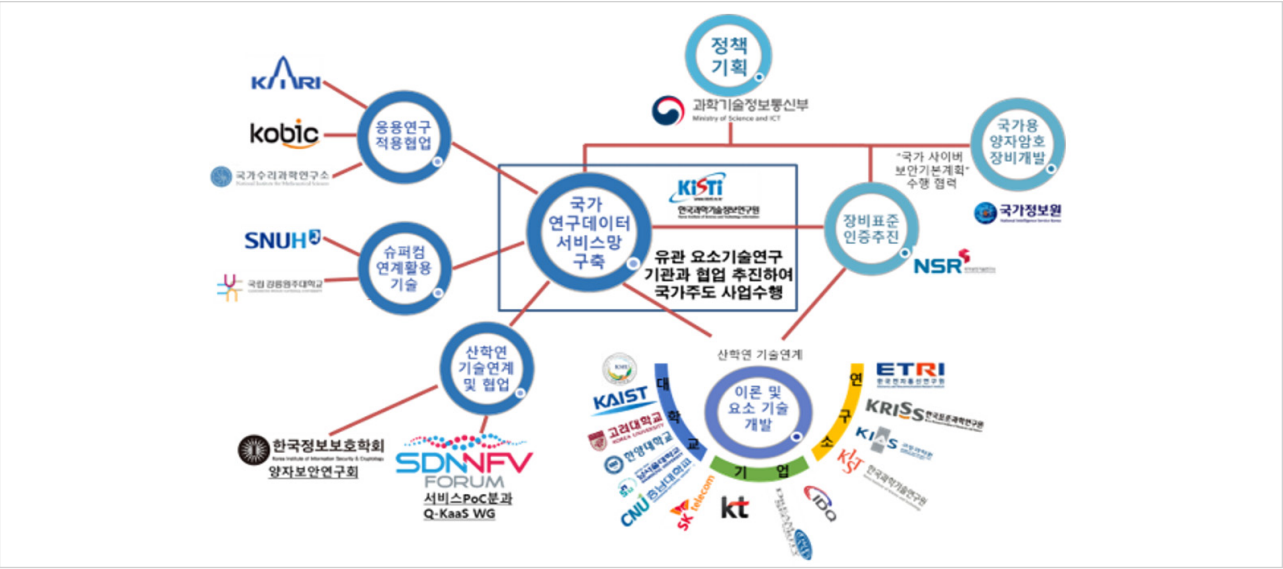
  - 국가 시범 공인 검증을 통한 개발 장비에 대한 보안 및 기능 검증 수행

- **(3단계) 거대과학연구분야 KREONET 양자암호통신망 구축 유스케이스 도출 및 양자암호통신망 인프라 서비스 관리 체계 수립**

  - 다 기관 양자암호통신망 구축을 통한 KREONET 적용 준비
  - 양자통신 실험 적용을 위한 시간동기화 및 위상보상기술 연구
  - 거대 과학연구분야 대상의 양자암호통신 연구망 서비스 응용사례 도출 및 국가 단위 양자암호통신 인프라/서비스 활용체계 수립 추진

양자암호기술 활용을 위한 대외 협력체계

<그림 4> KISTI 양자암호통신 연구협력 체계



- KISTI의 양자암호통신 연구 및 활용을 위한 대외 연구협력체계를 구성하여 산학연과 정부기관 등의 협력 추진 체계로 진행

- 한국정보보호학회를 통한 양자보안연구회를 설립하고, 양자암호 관련 연구개발 동향 및 연구결과 공유를 통하여 연구결과에 대한 객관성, 보안성 등에 대한 협업 추진

- 양자암호통신 관련 국내 표준화 동향 공유 및 추진을 위해 SDN/NFV 포럼에서 Q-KaaS (Quantum Key as a Service) 워킹그룹을 구성하여, 국내 산학연 연구진과의 표준화에 대한 협의를 통하여 객관화된 표준 내용 협의 추진

- 미래양자융합포럼 활동을 통하여 국내 양자암호통신 연구 활동에 대한 협력 및 과학기술계의 실제 양자암호통신망 구축을 위한 선도적 역할 추진

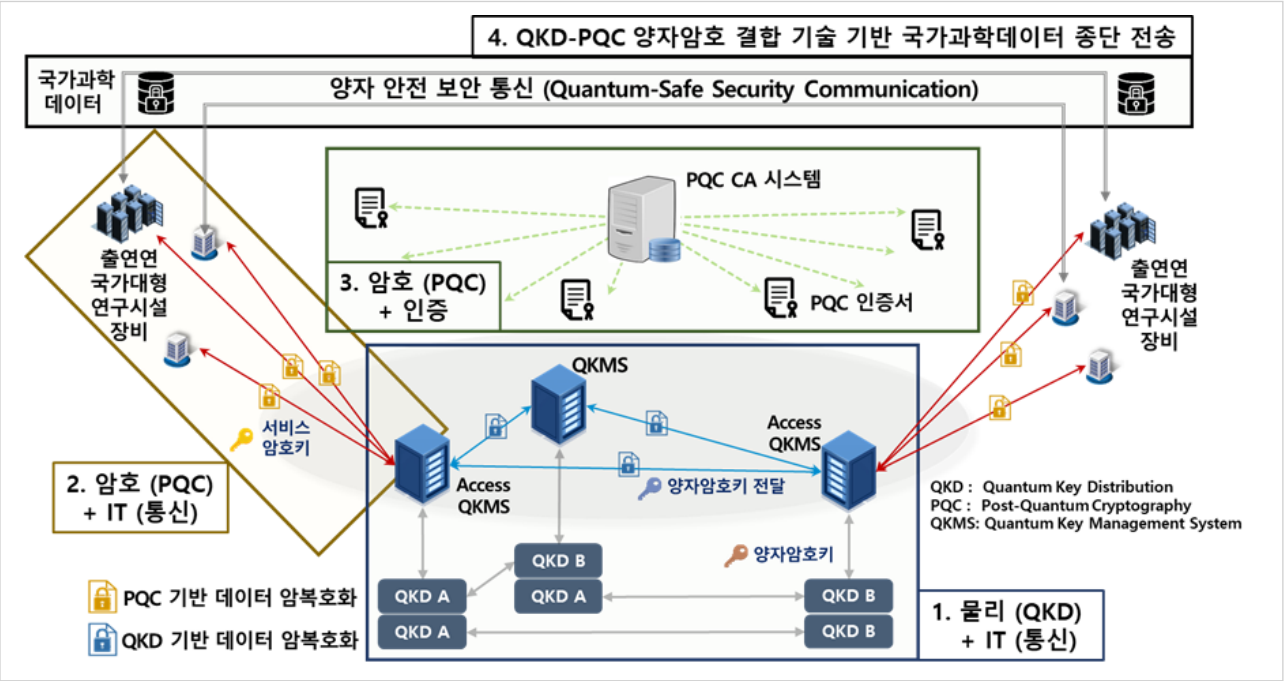
- 국가정보원, 국가보안기술연구소 등에서 추진하는 보안적합성에 대한 가이드라인 준수 및 협력체계로 개발 연구방향에 대한 국가 정책과 이슈에 부합되도록 추진

- 활용 대상이 되는 국가 중요 연구데이터를 이용하는 연구기관 등에 대하여, 각 기관의 전송환경 및 보안구성의 협조와 이해를 통한 사전 적용연구 방안 협력

- 산학연 등 양자기술 연구개발 기관과의 협력을 통하여 양자 요소기술별 활용과 협력을 통하여 통합 양자암호 통신망 구현 및 서비스 방안 협력

국가과학데이터 양자암호 인프라 전환 방안

<그림 5> 국가과학데이터 양자암호 인프라 전환 방안(안)



- **(개요)** 국가대형연구시설장비 등의 국가주요시설물에서 생성된 국가과학데이터의 양자 안전 보안 통신을 위하여 다음과 같은 양자암호 인프라 전환 계획을 추진함 : 1) 국가과학데이터 인프라 코어구간 QKD 기반 데이터 암·복호화, 2) 국가과학데이터 인프라 액세스구간 PQC 기반 데이터 암·복호화, 3) 국가과학데이터 인프라 양자암호 인증체계 구축, 4) 국가과학데이터 양자암호 인프라 환경 구축 및 출연연 대상 시범 적용·검증

- 높은 수준의 보안이 요구되는 국가과학데이터 특성상 무조건적인 안전성을 제공하는 QKD 중심의 양자암호 보안 체계 전환을 추진함

- 국가주요시설물 물리보안경계와 KREONET 양자암호통신망 액세스 구간의 PQC 기술 연계·적용을 통하여 양자암호 수준 보안성을 제고함

- 현재 데이터 암복호화에 편중된 국내 QKD, PQC 기술에서 탈피하고, 양자 기반 인증 부문에 대한 연구개발을 포함하여 포괄적인 양자암호통신망 인증 체계 구축을 추진함

- 양자기술 기반의 고보안성을 보장하기 위한 상호보완적 양자암호통신 체계 구축을 통하여 국가과학데이터 장기간 보호를 위한 현실적인 양자암호 인프라·서비스 전환을 추진하고 출연연 대상 시범 적용·검증함으로써 포스트 퀀텀 시대의 국가적 주요 데이터를 선제적으로 보호하고자 함

참고문헌

- 과학기술정보통신부, 양자보안연구회워크숍, “양자기술 관련 추진 현황 및 방향” (2021.09)
- 정보통신기술진흥센터 주간기술동향 (2016.10)
- Adam M. Lewis and Petra F. Scudo, (2022) “Quantum communications infrastructure architecture: theoretical background, network structure and technologies.”, arXiv:2110.06762v2 [quant-ph]
- INI R&C 양자정보통신 최신동향 및 시장전망 보고서 (2018.04)
- Miralem Mehic et al. (2020) “Quantum Key Distribution: A Networking Perspective”, ACM Computing Surveys, 53, 5(96)
- “Quantum Key Distribution (QKD) ; Components and Internal Interfaces”, ETSI GR QKD 003 V2.1.1 (RGR/QKD-003ed2), 2018.
- S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, “Advances in quantum cryptography”, Adv. Opt. Photon. 12, 1012-1236, 2020.
- [Stephanie Wehner, David Elkouss and Ronald Hanson (2018). “Quantum internet: A vision for the road ahead”, Science 362, 303
- Yu-Ao Chen et al. (2021) “An integrated space-to-ground quantum communication network over 4,600 kilometres”, Nature 589, 214
- Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. “Secure quantum key distribution with realistic devices”, Rev. Mod. Phys. 92, 025002, 2020.

KISTI ISSUE BRIEF의 내용은 KISTI의 공식적인 의견이 아닌 집필진의 견해이며 동 내용을 인용 시 출처를 밝혀야 합니다.

저 자 **김 용 환**
KISTI 과학기술디지털융합본부
과학기술연구망센터
양자n차세대연구망팀 선임연구원
T. 042-869-0899
E. yh.kim086@kisti.re.kr

이 원 혁
KISTI 과학기술디지털융합본부
과학기술연구망센터
양자n차세대연구망팀 책임연구원
T. 042-869-0648
E. livezone@kisti.re.kr

KISTI ISSUE BRIEF 제48호

발 행 일 2022. 10. 24.
발 행 인 김재수
편 집 위 원 조민수, 최희석, 이준, 정한민, 함재균, 이준영, 이상환, 곽영
발 행 처 34141 대전광역시 유성구 대학로 245
한국과학기술정보연구원 정책연구실
https://www.kisti.re.kr
I S S N 2635-5728

KISTI ISSUE BRIEF는 국가 과학기술 정보 분야 대표기관인 KISTI가 최근의 과학기술 정보 관련 현안·이슈를 발굴·분석하여 시사점 및 해결 방안을 제시하고자 발간합니다.