양자정보통신표준화 현황 및 전망

2021. 11. 12 | 김형수

PEOPLE. TECHNOLOGY. kt

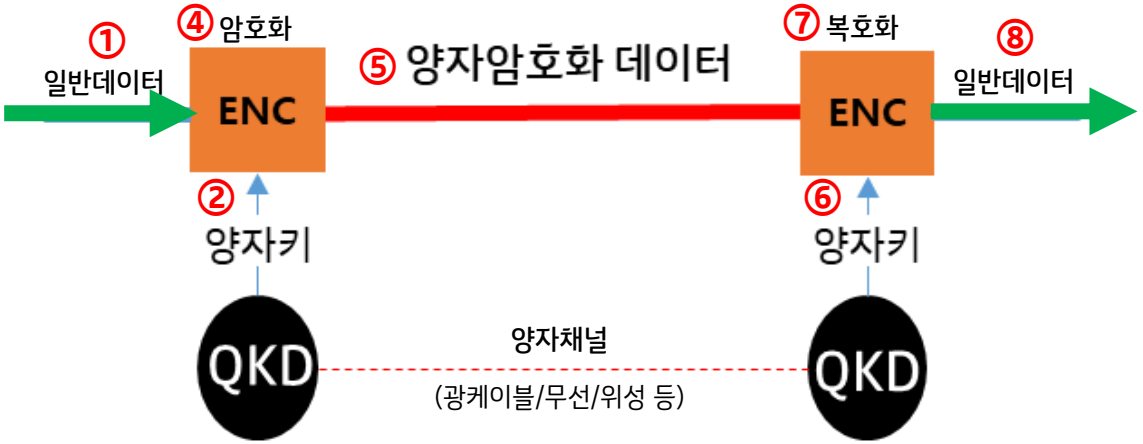
PEOPLE. TECHNOLOGY. kt Quantum

양자기술을 응용하여 안전한 암호를 생성하고 전달하는 기술

암호화 장치
(Encryptor)

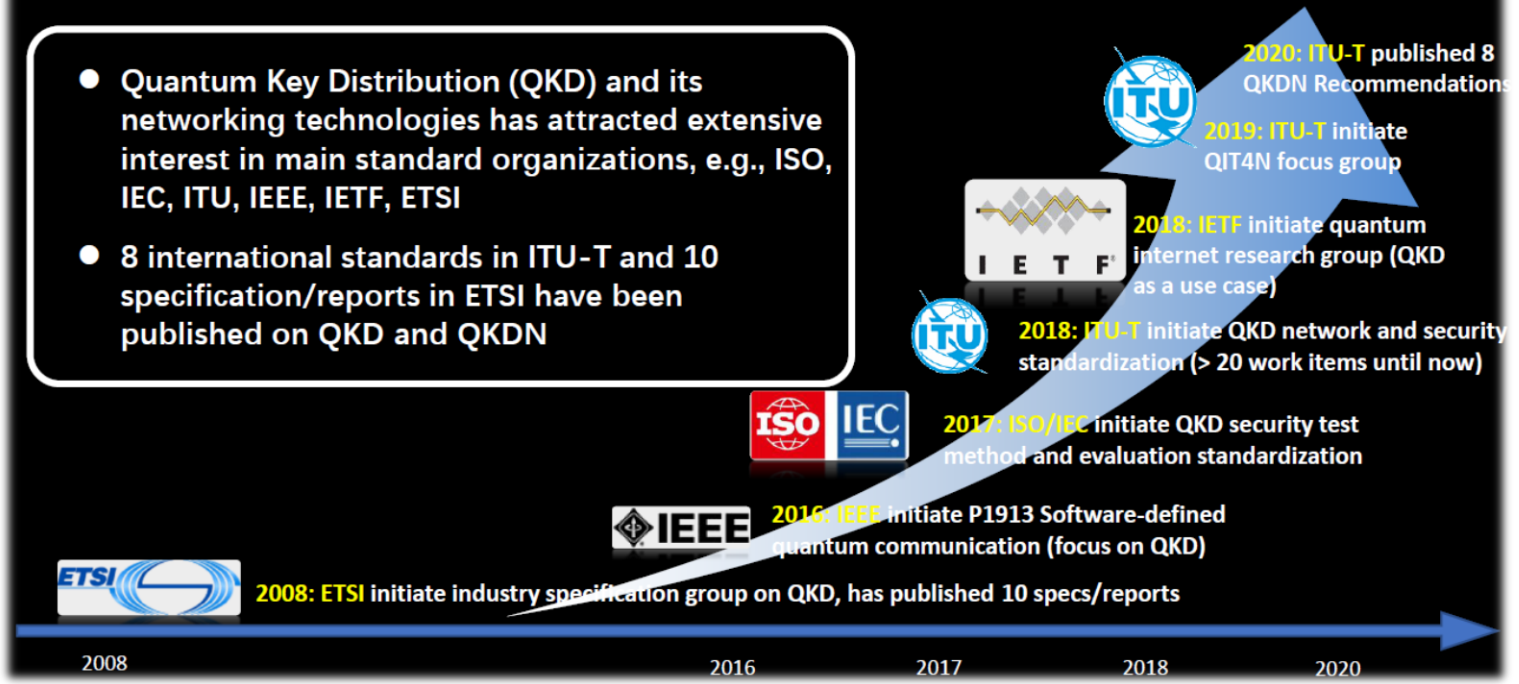
+

양자키분배 장치
(Quantum Key Distribution System)



Standardization on Quantum Key Distribution - Overview

- Quantum Key Distribution (QKD) and its networking technologies has attracted extensive interest in main standard organizations, e.g., ISO, IEC, ITU, IEEE, IETF, ETSI
- 8 international standards in ITU-T and 10 specification/reports in ETSI have been published on QKD and QKDN



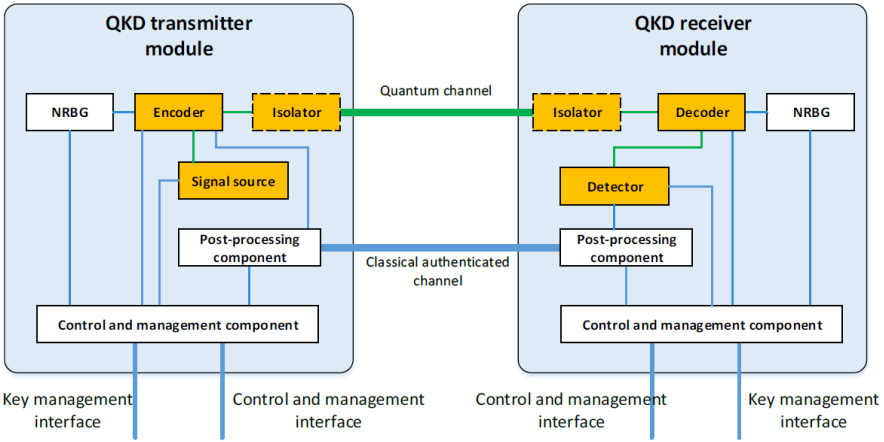
QKD 기술의 보안성 검토 → QKD 구현요소 표준화 → QKD 네트워크 요소기술 추가

ETSI GS QKD 015 V1.1.1 (2021-03)	Quantum Key Distribution (QKD); Control Interface for Software Defined Networks
ETSI GS QKD 004 V2.1.1 (2020-08)	Quantum Key Distribution (QKD); Application Interface
ETSI GS QKD 012 V1.1.1 (2019-02)	Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment
ETSI GS QKD 014 V1.1.1 (2019-02)	Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API
ETSI GR QKD 007 V1.1.1 (2018-12)	Quantum Key Distribution (QKD); Vocabulary
ETSI GR QKD 003 V2.1.1 (2018-03)	Quantum Key Distribution (QKD); Components and Internal Interfaces
ETSI GS QKD 011 V1.1.1 (2016-05)	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems
ETSI GS QKD 005 V1.1.1 (2010-12)	Quantum Key Distribution (QKD); Security Proofs
ETSI GS QKD 008 V1.1.1 (2010-12)	Quantum Key Distribution (QKD); QKD Module Security Specification
ETSI GS QKD 004 V1.1.1 (2010-12)	Quantum Key Distribution (QKD); Application Interface
ETSI GS QKD 002 V1.1.1 (2010-06)	Quantum Key Distribution (QKD); Use Cases
ETSI GR QSC 006 V1.1.1 (2017-02)	Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes
ETSI GR QSC 004 V1.1.1 (2017-03)	Quantum-Safe Cryptography; Quantum-Safe threat assessment
ETSI GR QSC 003 V1.1.1 (2017-02)	Quantum Safe Cryptography; Case Studies and Deployment Scenarios
ETSI GR QSC 001 V1.1.1 (2016-07)	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework
ETSI TR 103 570 V1.1.1 (2017-10)	CYBER; Quantum-Safe Key Exchanges
ETSI TR 103 617 V1.1.1 (2018-09)	Quantum-Safe Virtual Private Networks

ISO/IEC JTC1 SC27 WG3

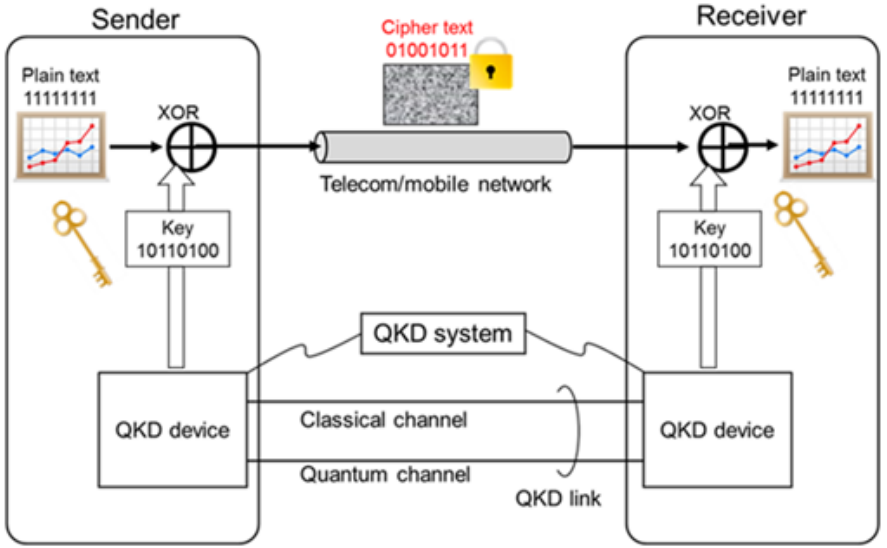
"WD 23837-1 : Security requirements, test and evaluation methods for QKD
- Part 1: Requirements"

"WD 23837-2 : Security requirements, test and evaluation methods for QKD
- Part 2 : Evaluation and testing methods"



Problem Statements

해외 주도 기술개발·표준화로 기술 종속성 & 과투자 우려



- 양자키분배 장치가 제공하는 기술 수용

  (연동 프로토콜, 암호키 공급 절차, 운용관리 정보 등)

- 통신 1회선/구간당 1세트의 양자키분배 장치 소요

- 양자기술력이 핵심 역량 & 성능

<ETSI; 유럽표준화기구>

3 ITU 국제표준화: 국제표준 확보

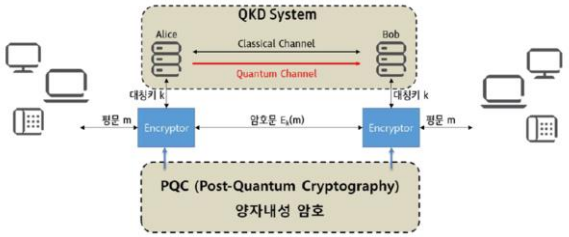
PEOPLE. TECHNOLOGY. kt Quantum

양자컴퓨터의 해킹 시도에도 안전한 보안 기술의 국제표준화 제안

- 양자키분배 장치가 제공하는 기술 수용
  (연동 프로토콜, 암호키 공급 절차, 운용관리 정보 등)
- 통신 1회선/구간당 1세트의 양자키분배 장치 소요
- 양자기술력이 핵심 역량 & 성능

KT, ITU 국제표준화 제안
- QKD 및 PQC 기술

(ITU-T SG17, 2017년)



INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG17-C180-R2

Study Group 17

Original: English

Question(s):	Q2/17, QAll/17	Geneva, 29 August - 6 September 2017

CONTRIBUTION

Source:	KT Corporation	
Title:	Proposal of new study on secure communication based on Quantum Cryptography	
Purpose:	Proposal	
Contact:	Jinmyung Lee KT corp. Republic of Korea	Tel:+82-10-7300-1297 Fax: +82-2-526-6306 Email: jmlee@kt.com
Contact:	Hyungsoo Kim KT corp. Republic of Korea	Tel:+82-10-6808-5199 Fax: +82-2-526-6306 Email:hans9@kt.com
Keywords:	ITU-T SG17, New Study, Quantum Cryptography, secure communication	
Abstract:	This contribution proposes to pro-active study on secure communication based on Quantum Cryptography.	

1. Introduction

At the last 3rd GSS (Global Standards Symposium) 16 meeting which was held in Hammamet, Tunisia, 24 October 2016, 'How industry meets end-users' expectations of security, privacy and

* ITU-T SG17; Security 표준그룹

4 ITU 국제표준화: 한국形 국제표준 확보

PEOPLE. TECHNOLOGY.

양자키분배 네트워크의 국제표준화 제안

- 양자키분배 장치가 제공하는 기술 수용
  (연동 프로토콜, 암호키 공급 절차, 운용관리 정보 등)
- 통신 1회선/구간당 1세트의 양자키분배 장치 소요
- 양자기술력이 핵심 역량 & 성능

KT, ITU 국제표준화 再제안
- QKD network 기술

(ITU-T SG13, 2018년)

INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2017-2020

SG13-C0509
Study Group 13
Original: English

Question(s): 16/13 Geneva, 16-27 July 2018

CONTRIBUTION

Source:	KT Corp.	
Title:	New: Proposal of a new work item on "Framework for Quantum Key Distribution Network"	
Purpose:	Proposal	
Contact:	Hyungsoo Kim KT corp. Republic of Korea	Tel:+82-10-6808-5199 Fax: +82-2-526-6306 Email:hans9@kt.com
Contact:	Jaehwan Jin LG Uplus corp. Republic of Korea	Tel:+82-10-8080-8167 Fax: +82-2-6928-8043 Email:daenamu1@lguplus.co.kr
Contact:	Sung Moon KIST Republic of Korea	Tel:+82-10- Fax: +82-31-546-7472 Email:s.moon@kist.re.kr
Contact:	J.-K. Kevin Rhee KAIST Republic of Korea	Tel:+82-10-6788-2814 Fax: +82-42-350-7416 Email:rhee.jk@kaist.ac.kr
Contact:	Gwangyong Yi Telefield, Inc. Republic of Korea	Tel:+82-10-9459-2031 Fax: Email: gwangyong.yi@telefield.com
Contact:	Jeongyun Kim ETRI Republic of Korea	Tel:+82-10-2461-3129 Fax: Email: jykim@etri.re.kr
Contact:	Junghyun Baik EYL, Inc. Republic of Korea	Tel:+82-10-3168-1418 Fax: +82-505-044-4445 Email: jhbaik@eylpartners.com
Keywords:	New Work Item, Quantum Cryptography, QKD (Quantum Key Distribution),	

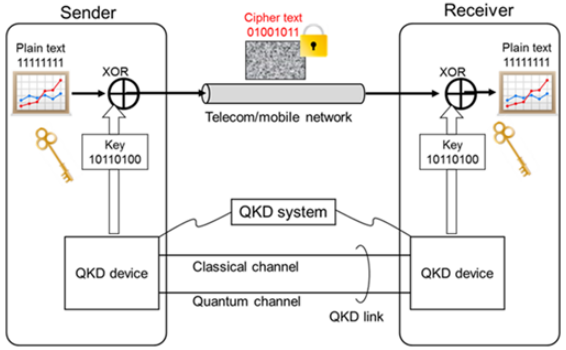
* ITU-T SG13; Future Networks 표준그룹

PEOPLE. TECHNOLOGY. kt Quantum

시스템 기술경쟁에서 네트워크 기술경쟁으로 Global Trend 전환

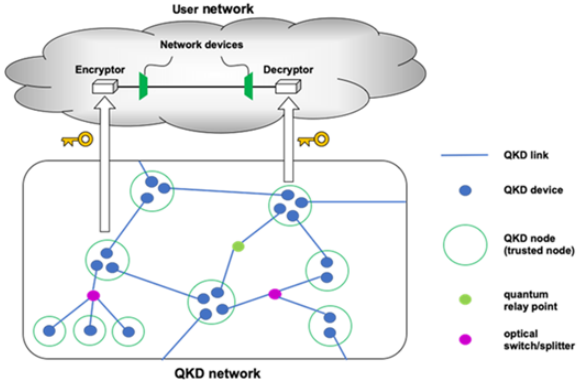
* ITU-T Rec. QKDN-FR 개발 착수 이후, ETSI도 QKD 네트워크 표준화 시작

(QKD system)



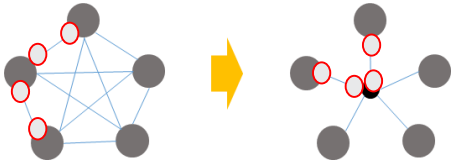
Device-centric 표준/ETSI

(QKD network)



Network-centric 표준

구간당 1세트; 10세트 소요



Overlay QKD망; 5세트 소요

ITUNews

Subscribe Topics About

New ITU standard for networks to support quantum-safe encryption and authentication

"To date, QKD systems have shared keys between two parties connected by a point-to-point QKD link," says Hyung-Soo Kim of KT, the lead editor of ITU Y.3800. "ITU Y.3800 extends these point-to-point links to a multi-point QKD network with a layered structure and standardized interfaces, supporting cost-effective QKD deployment, operation and maintenance."

6 ITU 국제표준: ITU-T Y.3800

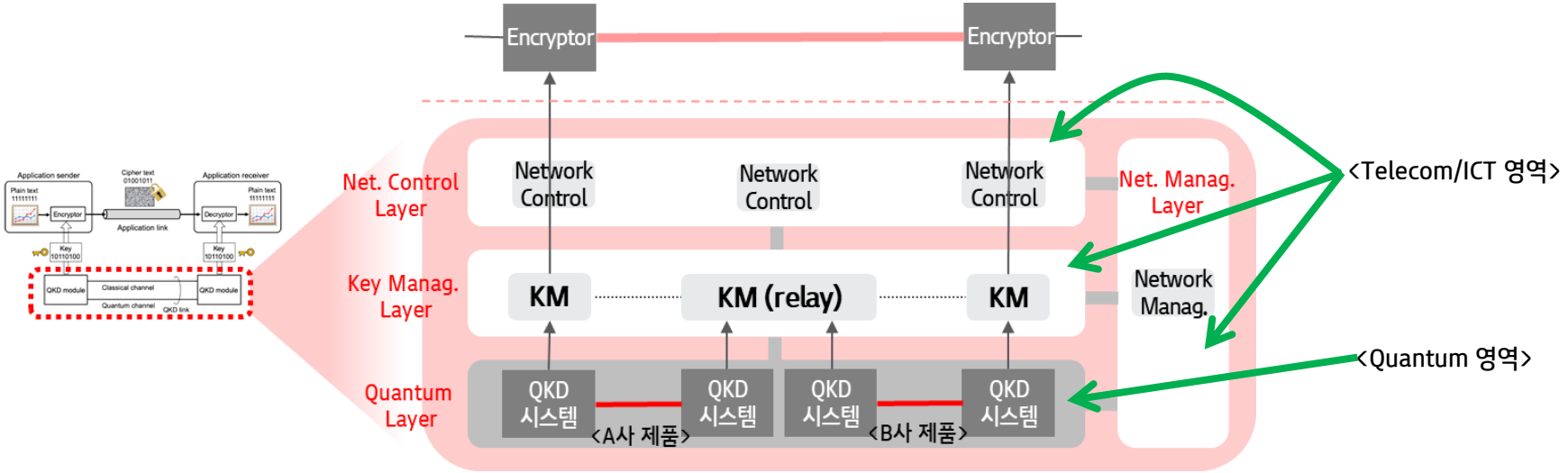
PEOPLE. TECHNOLOGY.

개방형 계층 구조로 기술종속 회피 및 한국形 기술선점 기회 확보

- 양자키분배 장치가 제공하는 기술 수용
  (연동 프로토콜, 암호키 공급 절차, 운용관리 정보 등)

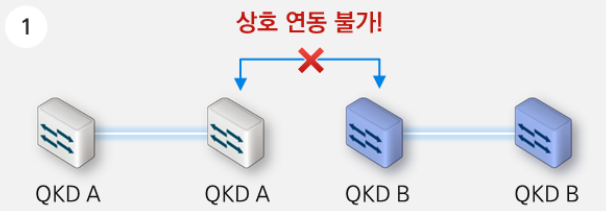
- 통신 1회선/구간당 1세트의 양자키분배 장치 소요

- 양자기술력이 핵심 역량 & 성능

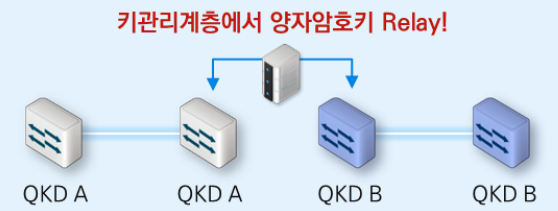


<ITU Y.3800>

1 QKD 이종 벤더간 연동 불가능
2 Over Spec 장비로 과다비용 발생



1 키 관리 계층에서 멀티 벤더 연동 지원
2 맞춤형 Spec 장비로 비용 효율화



* 256 AES/LEA/ARIA용 암호키 갱신 주기; 1분/1회
(KISA 암호키관리 안내서, 2년을 넘기지 않아야…)

해외 제조사의 장비 중심 기술개발/표준화 트렌드를 개방형 네트워크 중심으로 전환

(KT, 전체 19개 QKD 네트워크 관련 표준 중 10개 주관 & SG13 완성 표준 7건 중 4건 주관)

<Y.3800 기반 QKD 네트워크 관련 표준개발 현황>

붉은색: KT 주관 vs. 푸른색: IDQ 주관, 회색: 중국 및 일본

SG13 (Future networks): 14개

- QKD 네트워크를 위한 구조 및 프레임 워크 (Y.3800)
- QKD 네트워크의 기능별 기술 요구사항 (Y.3801)
- QKD 네트워크의 구조 (Y.3802)
- QKD 네트워크의 키 관리 기능 (Y.3803)
- QKD 네트워크의 제어 및 관리 (Y. 3804)
- QKD 네트워크의 SDN 제어 (Y.3805)
- QKD 네트워크의 QoS 보장 요구사항 (Y.3806)
- QKD 네트워크의 QoS 파라미터 (Y.QKDN_qos_pa) : 21년말 승인 목표
- QKD 네트워크의 비즈니스 역할 기반 모델 (Y.QKDN_BM) : 21년말 승인 목표
- QKD 네트워크와 보안 네트워크 인프라 통합 프레임워크 (Y.QKDN_frint)
- QKD 네트워크의 QoS 보장을 위한 기능별 구조(Y.QKDN-qos-arc)
- QKD 네트워크의 기계 학습 기반 QoS 보장 요구사항 (Y.QKDN-qos-ml-req)
- QKD 네트워크의 다중 서비스 제공자간 연동 (Y.QKDN-iwfr)
- QKD 네트워크의 네트워크 안전성 (Y.QKDN-rsfr)

SG17 (Security): 6개

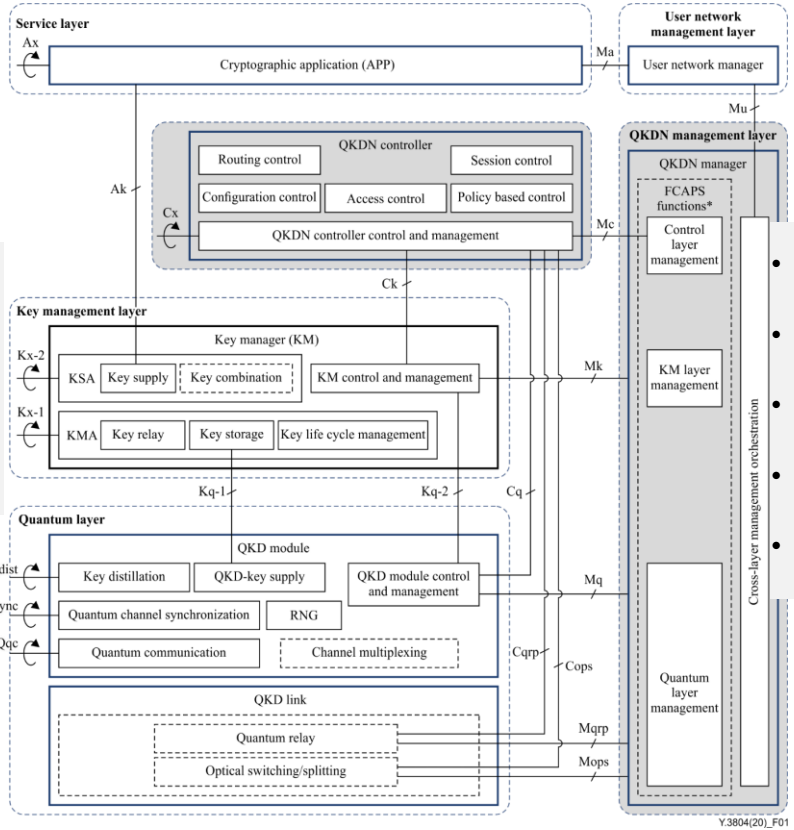
- QKD 네트워크의 보안 요구사항 – 개요 (X.1710)
- QKD 네트워크의 보안 요구사항 – 키 관리 (X.sec-QKDN-km)
- QKD 네트워크의 보안 요구사항 – 신뢰 노드 (X.sec-QKDN-tn)
- QKD 네트워크의 보안 요구사항 – 제어 및 관리 (x.sec-QKDN-cm)
- QKD 네트워크에서 생성된 키의 암호학적인 사용 (X.1714)
- 양자 잡음 난수 생성기 구조 (X.1702): 최종승인/'19.11
- 기술보고서 – 통신 네트워크에서 QKD를 위한 보안 프레임워크 (TR.sec-qkd)

8 양자암호 네트워크 제어 및 관리 (Y.3804)

PEOPLE. TECHNOLOGY.

Fault, Configuration, Accounting, Performance & Security 관리

- Routing Control: 경로제어
- Configuration Control: 구성 제어
- Policy-based control: 정책 제어
- Access Control: 접속 제어
- Session Control: 세션 제어



- Fault Management: 채널/링크/장비 장애 관리
- Configuration Management: 네트워크 구성 관리
- Accounting Management: 서비스 제공 관리
- Performance Management: 성능/품질 관리
- Security Management: 보안성 관리

9 양자암호통신 시스템 국산화

PEOPLE. TECHNOLOGY. kt Quantum

자체 기술개발 후 중소기업 기술이전 & 국산 상용시스템 확보

<독립형 Encryptor 자체 기술개발>

<중소기업 상용제품化; 코위버>

<연구용 QKD 자체 개발>

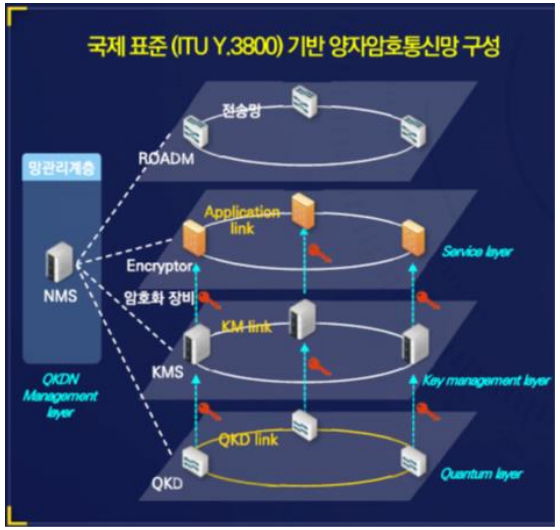
<중소기업 상용제품化; 코위버/우리넷>

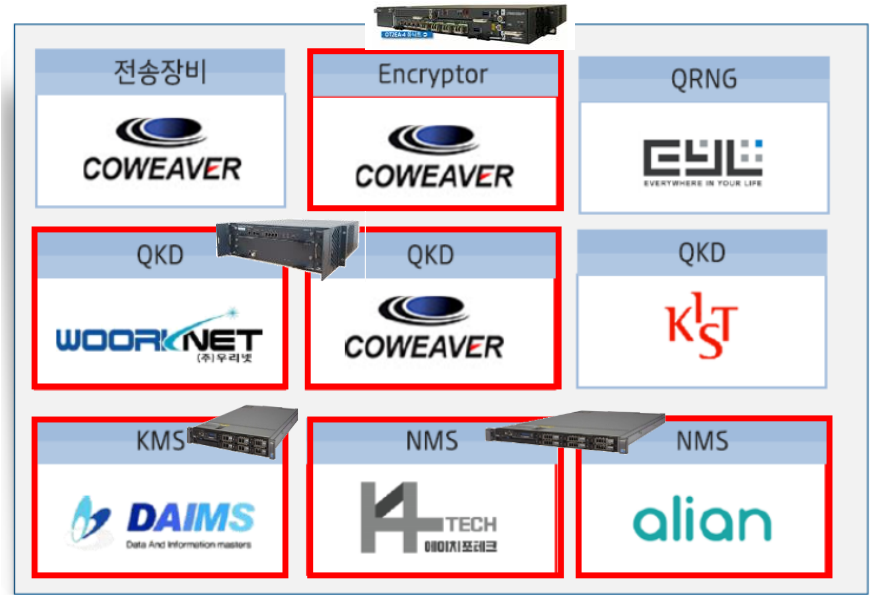
10 디지털 뉴딜 양자암호 시범인프라 구축 사업 ('20 ~) - 1

PEOPLE. TECHNOLOGY. kt Quantum

ITU 표준 기반 요소 시스템 개발 & 솔루션화

※ 국가 중요보안의 기술독립 & 100% 국내 생태계





: KT 기술이전/지도 제품

11 디지털 뉴딜 양자암호 시범인프라 구축 사업 ('20 ~) - 2

PEOPLE. TECHNOLOGY.

ITU 국제표준에 따른 구조/장비 구축으로 Reference 확보

※ 국가 보안 시설 & 핵심 산업인프라 적용

※ 양자암호 네트워크 모니터링 센터

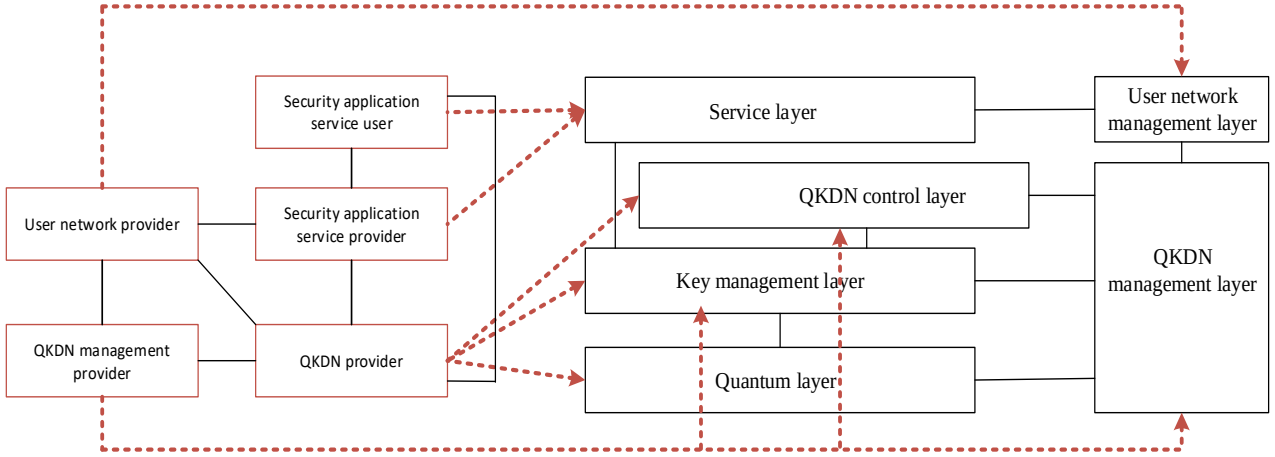
해외 제조사의 장비 중심 기술개발/표준화 트렌드를 개방형 네트워크 중심으로 전환

개방형 네트워크 역량을 바탕으로, 안정적 고품질 서비스 제공 준비 박차

양자암호 네트워크 비즈니스 모델 (Y.QKDN_BM)

Y.3800 기반 개방형 네트워크 구조에서, 시장 이해관계자간 biz model 정립

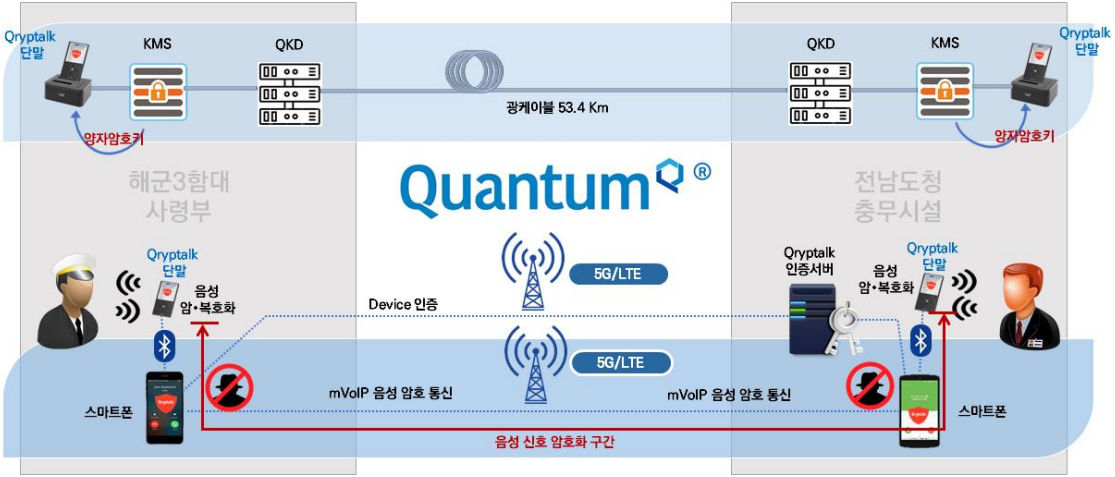
※ 장비 제조업체 外 국내 서비스 생태계 활성화



Quantum-비화통신: 세계최초 'QRNG + QKD' 양자암호화 통화서비스

- 양자암호키 연동 비화기 단말로 개인 또는 조직간 mVoIP 통신 서비스 제공
- 충전 크래들 장착 시 양자암호키 주입/교체 및 mVoIP 양자암호화

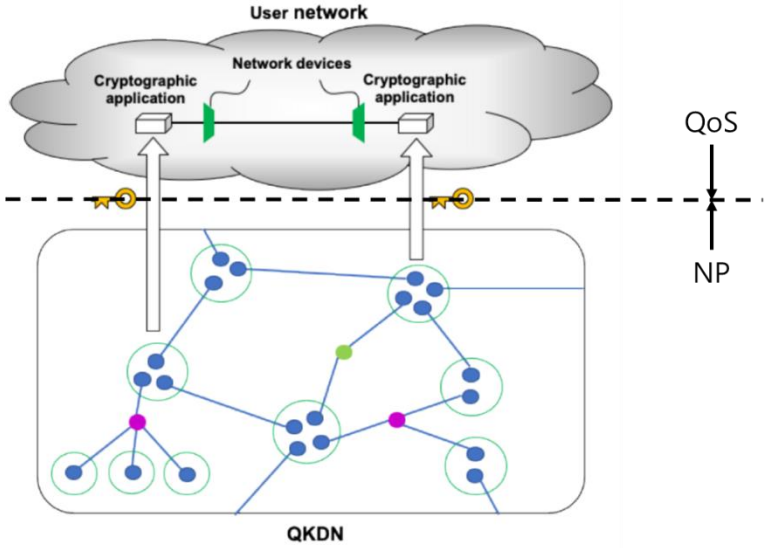
- QKDN provider; KT
- User Network provider; VoIP 사업자/구내망 운용자
- Security application service provider; EYL (국내 스타트업)



양자암호 네트워크 QoS 파라미터 (Y.QKDN_qos_pa)

서비스 이용자 측면에서의 양자암호 서비스 품질 평가 기준

※ 양자암호키 서비스 품질 관리 및 SLA 정립



(1) Throughput (처리율): 양자암호키 전달 량

(2) KKRD (응답 지연): 요청 시간 대비 양자암호키 도착 시간

(3) KKRDV (지연 변이): 예상 도착 시간 대비 실제 도착 시간

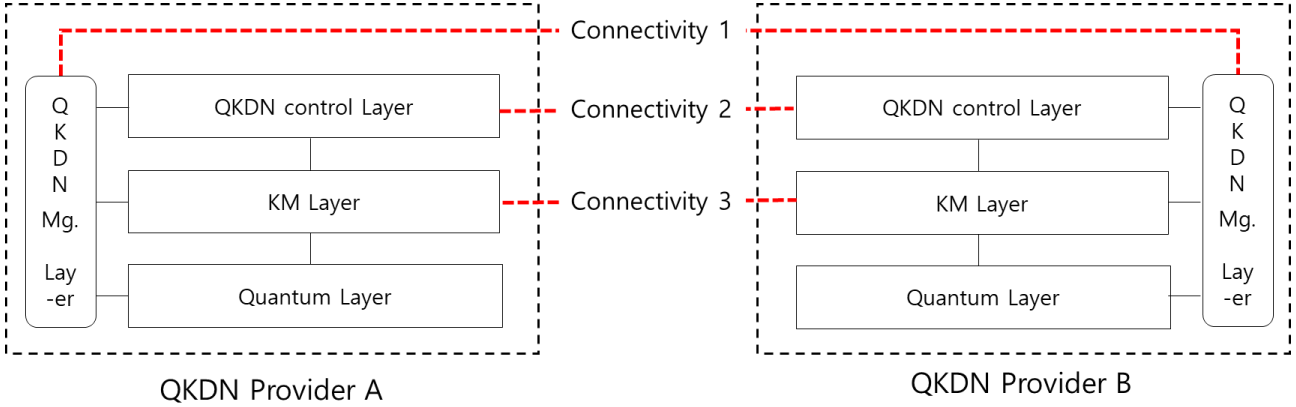
(4) KKER (에러율): 에러 발생 비율

(5) KKLR (손실율): 손실 발생 비율

(6) Availability (가용도): 품질평가 산정 가능 상태

양자암호 네트워크 Interworking (Y.QKDN_iwfr)

QKDN providers/Operators간 Multi-QKD networks 연동

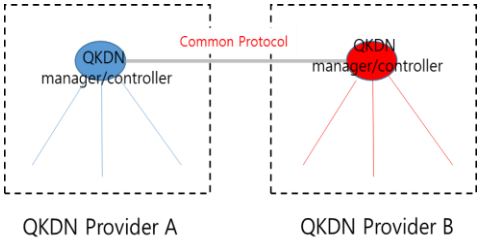


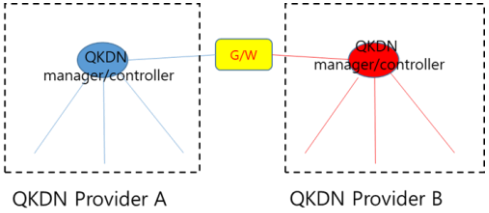
Connectivity 1) QKDN management layer interworking; QKDN management information should be shared between QKDN operators through QKDN management layer, such as fault, configuration, accounting, performance and security management.

Connectivity 2) QKDN control layer interworking; QKDN control information should be shared between QKDN operators through QKDN control layer, such as routing control, session control, authentication and authorization control and QoS policy control, etc.

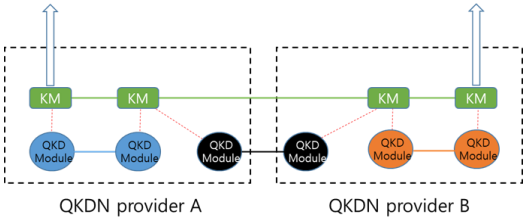
Connectivity 1) KM layer interworking; When QKD key relays between QKDN operators through KM layer, relative information for this purpose should be communicated, such as key ID, QKD module ID, key generation date, etc.

Connectivity 1 and 2

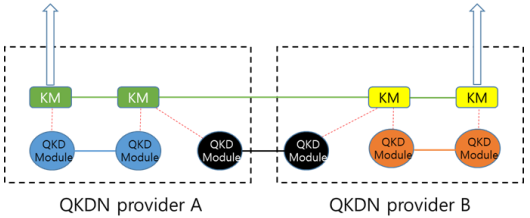




Connectivity 3

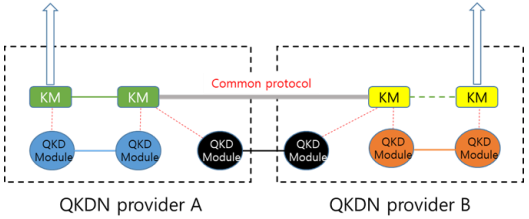


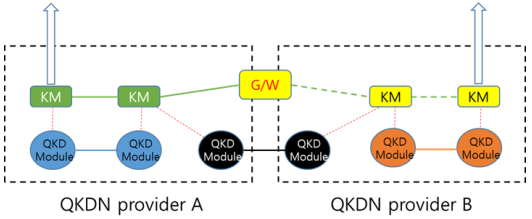
Homogeneous key manager and KM link protocol



Heterogeneous key manegers but homogeneous KM link protocol

Heterogeneous KMs and KM link protocols

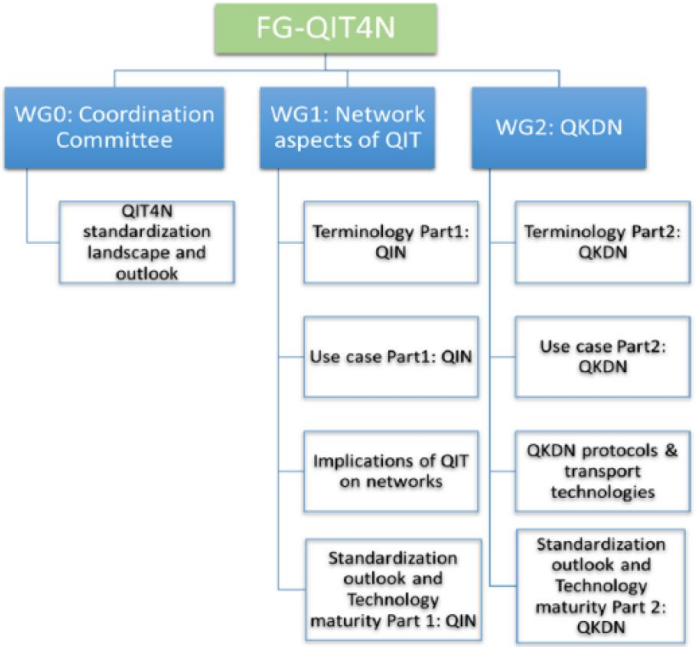




PEOPLE. TECHNOLOGY. kt Quantum

Focus Group on Quantum Information Technology for networks

- Established at ITU-T TSAG meeting in Geneva in 27 Sept. 2019.
- As a collaborative platform for pre-standardization of QIT for ICT networks
- It has held 9 meetings, 5 webinars and 2 joint activities in 2020-2021.
- Final Meeting:
  10th FG-QIT4N meeting
  E-meeting, 15 - 22 November 2021
- Participation: **Open and free to all interested stakeholders**



※ D2.2 Use Case 문서에 KT 사례 4건 반영

1 UC-6-1: QKDN for smart factory

1.1 Use case description

A commercial QKD network for smart factory is being deployed in Korea. This network applied QKD to leased-line between Hyundai Robotics and KT office in Daegu.

Hyundai Robotics manufactures industrial robots, applies them to overseas industrial facilities, and remotely operates through various ICT infrastructure such as IoT device, leased-line and servers. In this process, a malicious hacking threat on optical cable of leased-line may cause production disruption due to confidential leaks.

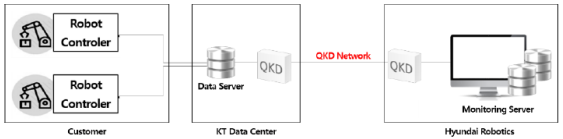


Figure 1-1. QKDN for smart factory

To prevent such problems, the QKD network is installed to protect corporate information and to enhance security.

<현대로보틱스 적용 Quantum-Robot>

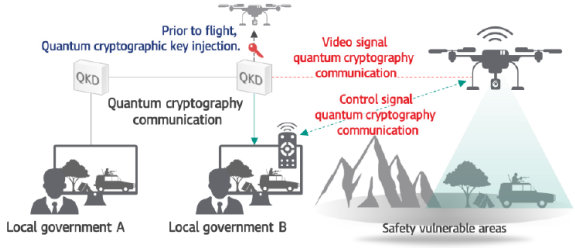


Figure 2-1. QKDN for social safety

By injecting the quantum encryption key supplied from QKD into the drone, not only the drone control signal is protected, but also the video signal from the drone is encrypted and protected to improve security.

2.2 Problem statement

Video data captured from flying Drone required the highest security is delivered to Local government. The wireless communication provides a connectivity between Drone and Local

<지상군작전사령부 적용 Quantum-Drone>

※ D2.5 Outlook 문서에 KT/한국 사례 다수 반영

Deployment	Span length (km)	Span loss (dB)	Channel	Method	Secure key rate (kbps)
	9 to 14.3				
Xi'an-Guangzhou	30/50	12.48/11.62	DF	DV	5.91/5.77
Zhucheng to Huangshan (Jinan-Qingdao)	66	~13	LF	DV	~3
KT corp. Gwangju to Gonjiam (5G commercial network)	15	6	LF	DV	0.01
KT corp. Bundang IDC to Su Court					
KT corp. 1st Digital New Deal national project (20					
KT corp. 2nd Digital New Dea					

Product	Features and parameters
QKD-based encryptor product #8	• Encryption layer: Layer 1, OTNsec • Client side interface: 1GE, 10GE, 100GE, OTU2/2e, OTU4, STM-1/4/16/64, 1G/2G/4G/8G/10G-FC • Line side interface: OTU2/2e, OTU4
QKD network provider #6	• Self-developed prototype of QKD-related systems and the technologies in 2020. Some technologies and products (KMS, NMS, etc.) are mostly ITU-T Y.38xx series-based. • Deployed and operated QKD networks on various areas; Governments, Factories, Medical canters, IDCs, 5G network, etc. Some iconic applications are Quantum-Drone for social safety, Quantum-Robot for smart factory environment, Quantum-DB for data centers, Quantum-Communication for secure mVoIP, etc.

<Field trials, Systems 및 사업자 소개>

6.2.9 Korea (Rep. of)

Quantum-ICT Technology Roadmap 2025 Report – For the overall Quantum Information Technologies (Quantum communications, Quantum sensing and Quantum computing), National Roadmap including the goal and direction was established. For the purpose of activation, the report introduced the actual strategy for R&D, man-power training, infrastructure development, etc.

Digital New Deal national project– A pilot project for building Quantum Key Distribution Networks in real field - was launched in 2020 by Korean government is in progress from 2020 to 2022. QKD-related national eco-system is expanding and verified the value of QKD technologies.

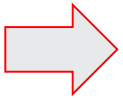
In June 2021, the amendment (focusing on Quantum Information technology) of the Information and Communication Convergence Act to foster the next-generation quantum industry was activated. It is a legal platform for the development of the quantum-related industry including human resources, international cooperation, R&D, field trial and the designation of a quantum cluster.

<한국의 주요 정책 및 현황>

QKD network

- 국내 생태계 글로벌 진출 및 기술 독립용 한국形 국제표준화: 한국, Global No.1 ITU 표준화
- 국내 기술 저변확대 위한 중소기업 기술 지원: ITU 표준 포함 기술이전 E2E 국산 솔루션化
- 국내 양자암호통신 산학연 기술 생태계 활성화: 16개 기업 신규 진입 & 디지털 뉴딜 참여

World First
QKD 서비스



World First
양자인터넷 서비스

PEOPLE. TECHNOLOGY.