[ONK 2019 Fall]

양자암호통신 서비스 인프라 기술 및 표준화

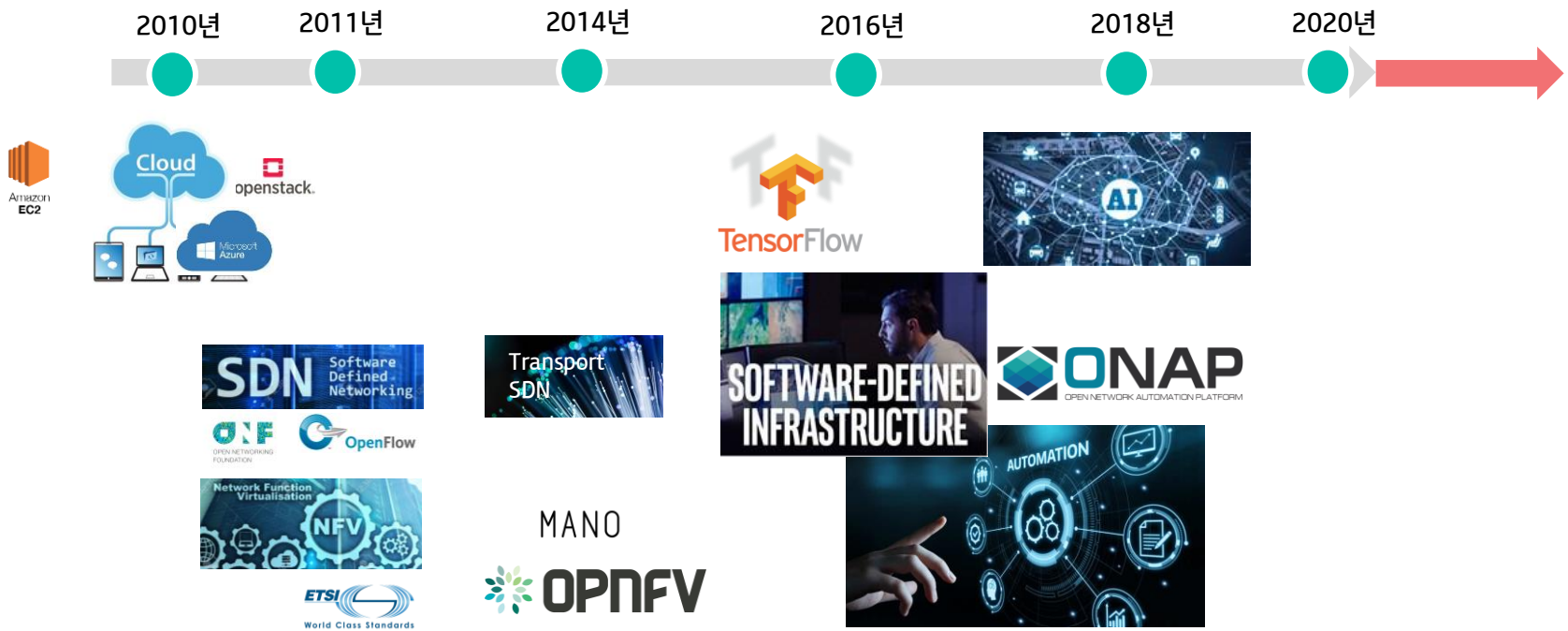
Make it Real.

2019. 11. 06 | 융합기술원 Infra 연구소

PEOPLE. TECHNOLOGY. kt

01 Intro

지난 10년 동안 가상화, 자동화, 지능화 관점의 기술진화와 인프라 변화가 진행되어 왔음. 향후 10년은??



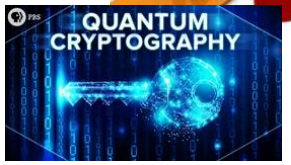
01 Intro

나는 무엇을 해 왔나? 또 앞으로 무엇을 할 것인가?

2010년 2011년 2014년 2016년 2018년 2020년

인프라전략
(SDN, 플랫폼)

향후 10년의 변화를
이끌 기술은???



01 Intro

양자기술에 대한 첫인상…

어렵다

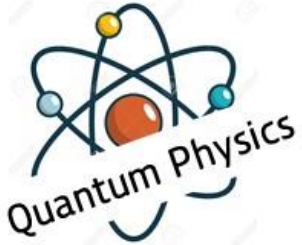
Qubit: 0과 1이 중첩???
측정? 확률?

실현가능하긴 해?

슈퍼 컴퓨터(1만년)
=> 양자 컴퓨터(3분20초)

나와는 상관이 없다.

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



02 Quantum

양자가 어렵다? 그냥 믿으면 쉬워진다…

양자(Quantum)란? : 물리적 성질을 이루는 불연속적인 최소 단위의 입자 또는 상태
예) 더 이상 나누어지지 않는 빛의 입자 = 광자

리차드 파인만(1918~1988, 미국)

"양자 역학을 이해하는 사람은 아무도 없다."

양자역학은? : 상식적으로 설명하기 힘든 원리를 설명하는 학문

이해란? 새로운 지식과 알고 있던 지식의 논리적인 연결

➔ 우리의 지식은 거시세계에서 얻어진 지식이고,
미시세계는 경험할 수 없기 때문에 이해하기 어렵다.

양자의 원리

① 중첩(Superposition) : 서로 구별이 가능한 2가지 상태가 동시에 존재

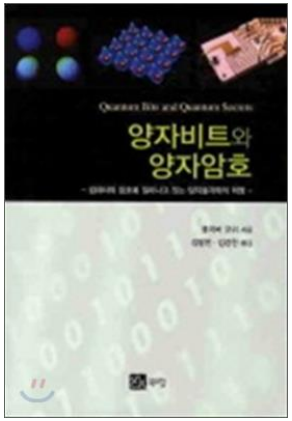
② 이중성(Duality): 입자의 성질과 파동의 성질을 동시에 가짐

③ 측정의 원리(복제불가능): 중첩이 되어 있는 양자는 측정하면 깨지고 변형됨

④ 불확정성(Uncertainty): 양자의 2가지 상태를 동시에 측정하는 것은 불가능, 확률로만 해석 가능

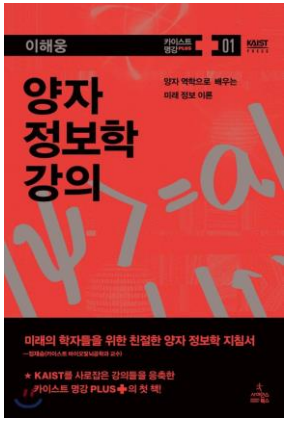
첨부Quantum

참고도서 및 자료



올리버 모쉬 저
/ 북스힐, 2010.5

Ishikawa Kenji 저
/ 성안당, 2017



이해웅
/ 사이언스북스, 2017.12

YouTube

양자통신 강의(online): 한양대 배준우 교수님

- http://www.kocw.net/home/cview.do?cid=a38c1c2fd0fa8989

03 Quantum Computer

Quantum Supremacy가 실현됐다??

양자우위 (quantum supremacy)란?

양자컴퓨터가 기존 최고 컴퓨터(수퍼컴퓨터)보다 우수한 성능 보인 순간
→ 현존하는 수퍼컴퓨터로 1만년 걸리는 수학 문제를
53qubit 양자 컴퓨터로 3분 20초 만에 푸는 데 성공

https://www.youtube.com/watch?v=vTYp5Kd9nMA

- **Google**
  > 2009년 '양자 인공지능(Quantum AI)' 연구 시작
  > 2013년 NASA와 공동으로 '양자 인공지능 연구소 설립. 범용 양자컴퓨터 연구개발 진행
  > 2019.9월, 자사 개발 양자컴퓨터가 "양자우위(quantum supremacy)를 달성"했다고 발표
- **캐나다의 디웨이브(D-Wave)사**
  > 2013년 'D-Wave 2' Google/NASA에 판매하며 시작
  > 2,048 qubit 시스템 보유. 5,000 qubit 개발중
- **IBM**
  > 양자컴퓨터 상용화 기술개발에 가장 앞선 기업 중 하나
  > 2016년 '퀀텀 익스피리언스(Quantum Experience, IBM Q)' 공개
  → 양자프로세서에서 프로그래밍과 다양한 테스트 가능
  > 2017. 5월에 상업용 프로토타입 17큐비트 양자컴퓨터 프로세서 공개
  > CES 2019에서 최초 상업용 양자컴퓨터인 IBM Q System One 발표
  > 19.9월 IBM Q Experience 플랫폼을 온라인으로 사용할 수 있는 53-Qubit 양자 시스템을 공개

첨부 양자암호통신 연구

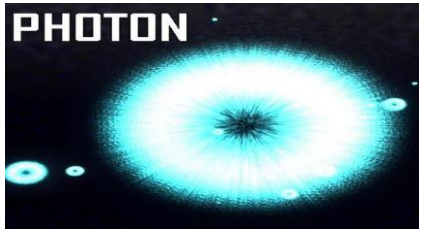
양자컴퓨터 대응을 위한 기술

암호화 방식	활용	암호체계 위협	대응 기술
공개키 방식 (소인수분해 등 수학적 계산상 난점을 활용한 방식)	암호통신을 하기 위한 상호간에 대칭키를 교환하기 위해서 사용	양자 컴퓨팅 일반컴퓨터가 수 백년에 걸쳐 풀어야만 풀 수 있는 소인수분해 계산을 단시간 안에 끝낼 수 있음. (300자리 소인수 분해에 슈퍼컴퓨터 1년, 양자컴퓨터 30분 소요*)	QKD (양자암호통신) 양자암호 통신을 이용해서 Key를 교환함
			Post-Quantum Cryptography 양자컴퓨터의 공격으로부터 안전한 암호알고리즘 (현재 연구 중)
대칭키 방식 (랜덤 값을 생성하여 활용한 방식)	실제 데이터를 암호화를 할 때, 사용하는 Key	컴퓨터 성능의 발전 랜덤의 패턴을 분석하기 보다는 짧은 시간에 모든 값을 대입해서 암호를 해독할 수 있음	암호화 BIT 크기를 증가 80bit : 2010년까지 112bit : 2030년까지 128~256bit : 2030년 이후 까지
		저사양 IoT 단말들 사양이 낮을 수록 생성할 수 있는 랜덤값의 범위가 적음. 즉, 80bit의 랜덤을 사용할 수 있음.	별도의 난수생성 모듈 사용(QRNG) 그러나, 현재 대부분 저사양 IoT 단말들도 128bit의 Key 생성 가능

04 양자암호통신 서비스

QKD가 생산한 암호키를 기존 통신 인프라에 제공하기 위해 필요한 경로제어, 자원제어, 암호키할당 등 네트워킹 기술이 필요

양자



QKD 장치: **암호키 생성/분배**

> 아주 약한 빛(Photon)을 이용
> Random한 편광판을 이용하여 0/1 신호 전송
> 사용한 편광판 정보 교환
> 양단간 일치 정보를 이용하여 암호키 생성

QKD Layer

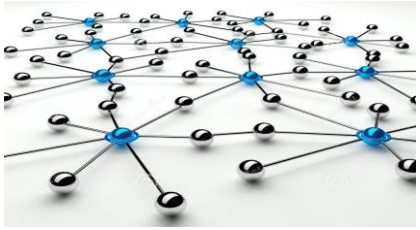
암호Network

QNC 장치: **암호키 네트워킹**

> 암호키 관리; 분할, 저장, 할당, Sync
> E2E 암호키 네트워킹: Unicast, Multicast
- Key routing, 자원예약
> Monitor.: Key 자원품질, 장애, 진단/제어

Quantum NW Layer

통신서비스



암호통신서비스: **암호키 사용**

> 암호방식: 기존 암호알고리즘 사용(AES, RSA…)
> 통신장비(L1~L4) 또는 응용서비스
- WDM, P/OTN, L2, L3, Application
> 암호화기(Encryptor)로 평문을 암호화

NW Layer

05 양자암호통신 인프라

양자암호통신서비스를 제공하기 위한 인프라

Key 생성(QKD)

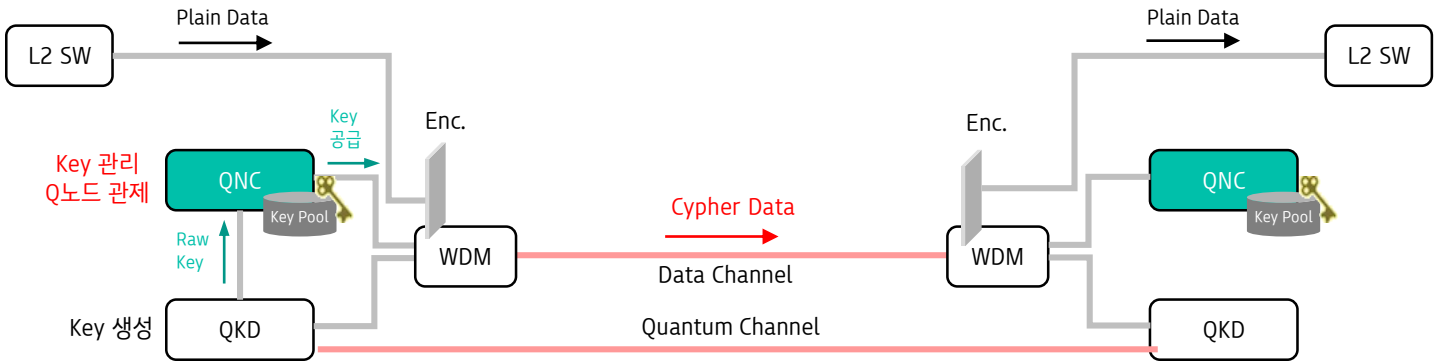
-- 송신측
① QRNG로 난수 생성(송신측 위상 결정)
② 약한 광을 위상변조로 인코딩&송신
-- 수신측
③ QRNG 난수 생성(수신측 측정 위상 결정)
④ 신호 디코딩
-- 송수신측 신호처리
⑤ 상호 위상교환 후 Key 확정

QKD Node 제어(QNC)

-- Key 공급
① Enc. 요청에 따른 Key 분할/공급
② QNC간 Key 분할정보 Sync
-- Q-Node 관제
① Key 생성품질(Key rate, BER 등)관리
② QKD 장애/성능 감시
③ QKD 진단/제어

암호통신(Enc.)

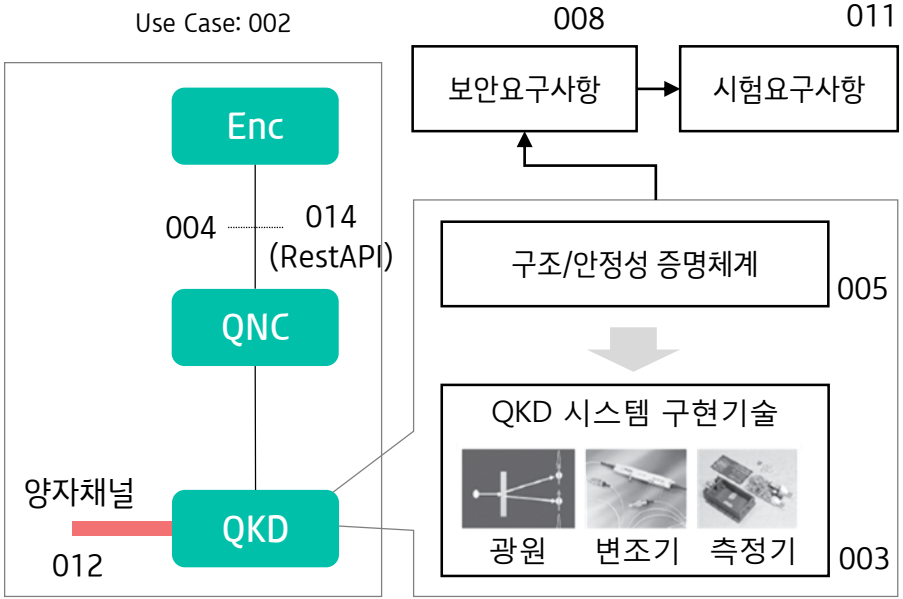
-- 송신측
① Plain Data 수신
② 암호방식 결정(AES, LEA, DES)
③ QNC에 Key 요청
④ Data 암호화 및 전달
-- 수신측
① 암호 Data 수신 및 복호화
② Data 전달



06 ETSI 표준화 동향

19.2월 QKD와 기존 통신인프라간 Key 전달과 관련된 인터페이스 표준이 발간됨

https://www.etsi.org/committee/qkd



번호	표준명	버전	발행일
014	Protocol and data format of REST-based key delivery API	1.1.1	19.02
012	Device and Communication Channel Parameters for QKD Deployment	1.1.1	19.02
007	Vocabulary	1.1.1	18.12
003	Components and Internal Interfaces	2.1.1	18.03
011	Component characterization: characterizing optical components for QKD systems	1.1.1	16.05
008	QKD Module Security Specification	1.1.1	10.12
005	Security Proofs	1.1.1	10.12
004	Application Interface	1.1.1	10.12
002	Use Cases	1.1.1	10.06

07 ITU-T 표준화 동향 - SG13

한국, 일본을 중심으로 5건의 document 표준화 진행중

https://www.itu.int/ifa/t/2017/sg13/docs/

표준문서	문서명	목표	Scope
Y.3800 (Y.QKDN_FR) ('19.6월 승인) > KT	Framework for Networks supporting Quantum Key Distribution	표준기술 관점에서 사용자 네트워크와 QKD 네트워크를 구성/구축/운용하기 위해 필요한 요소들을 제시	> QKD 기술 개요 > 사용자 네트워크와 QKD 네트워크의 관계 > QKD 지원을 위한 네트워크 요구사항 > QKD네트워크의 개념적 구조와 기본기능
Y.QKDN_Arch (19.5월 제안) > China / NICT	Functional Architecture of the Quantum Key Distribution Network	QKD 네트워크의 디자인 원칙 제시 - Functional architecture model, 기능요소, 인터페이스, 설정, 운영절차	> Y.3800에 정의된 일반 구조를 기반으로 QKD 네트워크 아키텍처 정의
Y.QKDN_KM (19.5월 제안) > NICT	Key management for Quantum Key Distribution Network	QKD 네트워크의 키 관리 제시	> 양자암호키 관리 요구사항 > 기능 요소 (Functional elements) > 키관리 절차 > Key formats (key data and meta-data)
Y.QKDN_SDNC > China (Beijing Univ.)	Software Defined Network Control for Quantum Key Distribution Networks	QKD 네트워크에 대한 SDN 제어	> Q-SDN 기능 요구사항 > SDN 기반 제어 구조 > 계층적 SDN 컨트롤러
Y.QKDN_CM > ETRI, KT	Control and Management for Quantum Key Distribution Network	QKD 네트워크에 대한 제어/관리	> M&C의 기능 요구사항 > M&C 구조 > Management information model > Multi-layer 환경에서 M&C Orchestration

07 ITU-T 표준화 동향 - SG17

한국, 일본을 중심으로 5건의 document 표준화 진행중

표준문서	문서명	목표	Scope
TR.sec-qkd (18.8제안) > SKT	Security framework for quantum key distribution in telecom network	통신 사업자 관점의 요구사항을 만족시키는 QKD에 대한 보안 프레임웍	> 네트워크에서 QKD security functions의 일반적 구조 > QKD 시스템과 암호화 App 사이의 위협/보안 functions > QKD 시스템과 관리/감시 시스템 사이의 위협/보안 functions > QKD 네트워크에서 양자암호 중계 기능
X.cf-QKDN ('19.6제안) > SKT	The use of cryptographic functions on a key generated in Quantum Key Distribution networks	QKD Key security와 Key 전달에 대한 안전성 검증 명세	> QKD가 생성한 키의 기존 암호화 표준 승인 가능화 > 기존 보안 표준에 따른 키 배포 승인 가능화
X.qrng-a ('19.9제안) > SKT	Quantum noise random number generator architecture	Quantum entropy source의 기능 구조	> Quantum entropy source에 대한 명세 > Quantum entropy source의 엔트로피 측정 방법 > 엔트로피 검증
X.sec-QKDN-km (19.9 제안) > NICT	Security requirements for QKD networks - key management	QKD 네트워크 상에서 KM의 보안 요구사항	> KM의 보안 위협 > KM의 보안 목표 > KM의 보안 요구사항 > 보안요구사항을 만족시키는 KM 명세
X.sec-QKDN-ov (19.9제안) > SKT	Security requirements for quantum key distribution networks - overview	QKD 네트워크 보안요구사항에 대한 개요	> QKDN의 보안 위협 > QKDN 운영 / trusted node 보안 요구사항 > 사용자 네트워크와 QKDN 사이의 security demarcation > Damage control and recovery

08 TTA 표준화(PG201) Direction

양자암호통신 서비스 기술 중, 네트워크 기술 및 키 관리 기술을 중심으로 표준화 진행

구분	표준화 대상 기술	표준화 범위
양자 	단일광자 송수신 기술	ETSI표준 준용
	광 신호처리 기술	
	양자암호 프로토콜 기술	
암호 	암호 기술	기존 암호 기술 활용
통신 	시스템화 기술(M&C, Data Model, API)	PG201 표준화 Direction
	네트워킹 기술	
	키 관리 기술	
	OTN Encryption	

[ONK 2019 Fall]

양자암호통신 전달네트워크 기능구조 표준

Make it Real.

2019. 11. 06 | 융합기술원 Infra 연구소

PEOPLE. TECHNOLOGY. kt

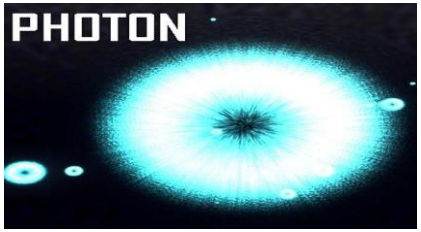
01 표준화 목적

종단간 양자암호 기반 통신서비스 제공할 수 있는 양자암호 전달네트워크 기능구조 정의

=> 양자암호통신 산업 생태계 활성화, 기술개발 및 관련 산업 장려

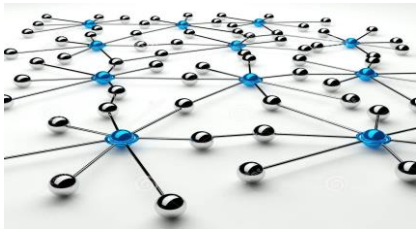
양자암호 전달네트워크 표준

QKD



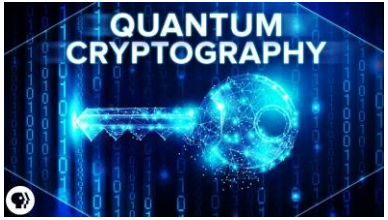
양자 암호키 분배

Transport Network



Data 전달

양자암호통신



종단간 양자암호통신

02 Scope

Trusted Node 기반 QKD 전달 네트워크 구현을 위한 표준화 추진

표준화 범위

Trusted Node 기반 QKD 전달 네트워크를 대상으로 하며 다음과 같은 범위로 한다.

> 기능구조 (Functional Architecture)
> 기능요소 (Functional Elements)
> 참조점 (Reference Points)
> 운영절차 (Operational Procedure)
> 보안 고려사항 (Security Considerations)

고려사항

Efficiency	효율적인 키 제공 & 전달 가능
Security	QKD 장치로의 Direct Control 방지/보안 방안 제공
Transparency	개방화된 인터페이스 제공
Interoperability	Multi-vendor interoperability 제공
Robustness	Node/Link Fail에 대한 fault detection & recovery
Policy Control	Flow별 QoS/Charging Policy Control/mgmt. 제공
Scalability	P2P, MP2MP 등 다양한 토폴로지 & 장거리 네트워크

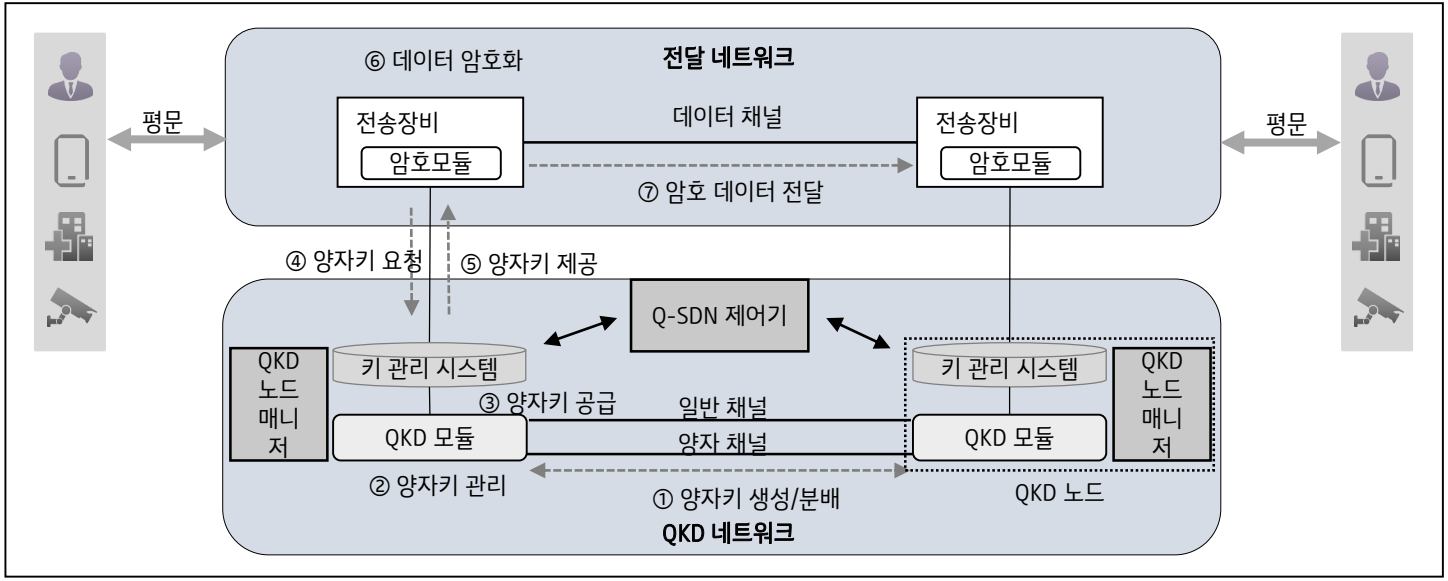
03 양자암호 전달네트워크

기존 전달장비에 암호모듈(Encryptor/Decryptor)을 추가하고, 암호화를 위한 Key를 QKD로부터 제공 받음

양자채널을 통해 생성된 암호키를 이용하여 E2E간 암호통신 수행

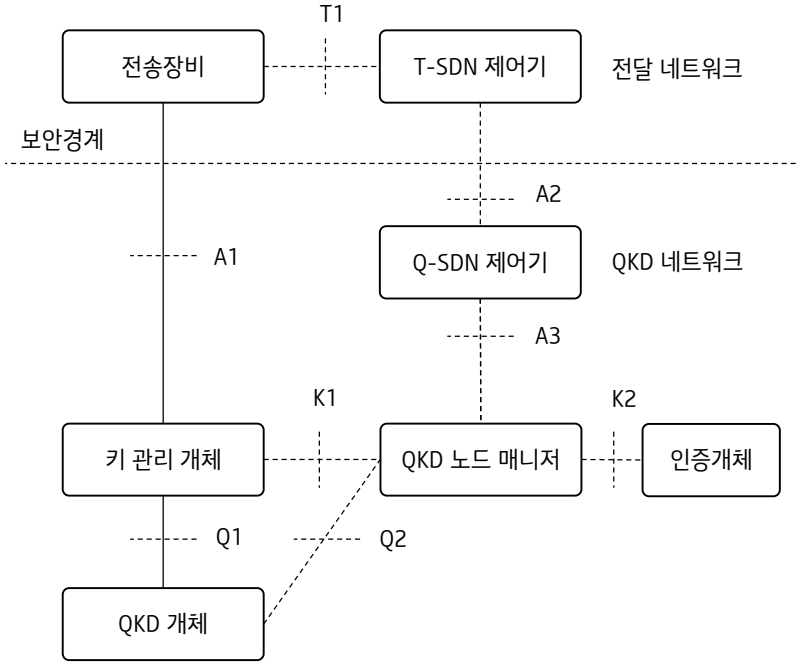
> QKD(Quantum Key Distribution): 암호키 생성

> Encryptor(Decryptor): 암호키를 이용한 평문데이터의 암복호화



04 Functional Architecture

Transport Network에 특화된 양자암호통신 네트워크 구조



[Functional Elements]

> **전송장비**: 기존 데이터 망의 전송장치. 예) POTN, ROADM

> **T-SDN 제어기**: 기존 데이터 망의 네트워크 제어기

- Q-SDN 제어기의 요청을 받아 기존 데이터망 자원 할당

> **Q-SDN 제어기**: QKD 네트워크 제어기

- QKD 네트워크 자원관리, QKD 네트워크 감시/제어 수행

> **QKD 노드 매니저**: Trusted Node 내 관리자

- Trusted Node 내 자원관리: 현황정보 수집, 장애감시, 진단/제어
- QKD 네트워크 정보관리: 포워딩 테이블(Address, Interface)

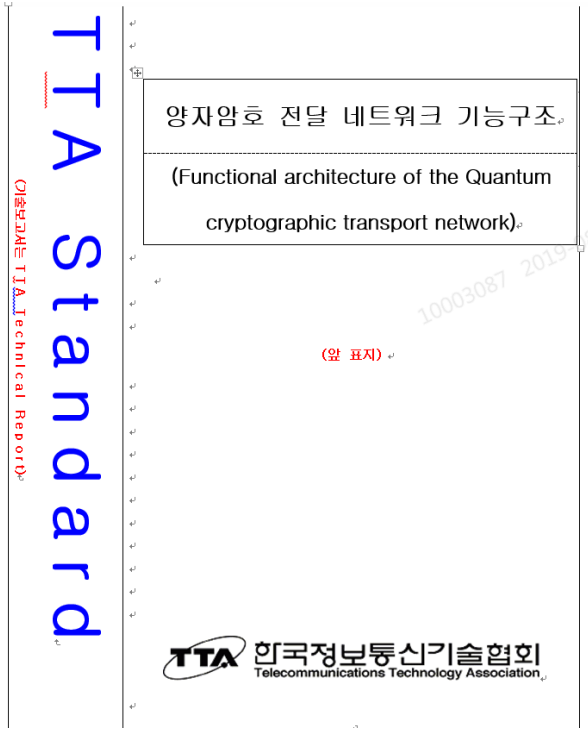
> **인증개체:** 클라이언트(or NE)에 대한 인증

> **키관리개체:** 양자암호키 관리

> **QKD 개체:** 양자암호키 생성

05 문서구조

'19.12월까지 표준화 완료 추진



06 ITU-T SG15 표준화

ITU-T SG15 Seoul interim meeting을 통해 표준화 Work item 제안. ITU-T 내 Focus Group 진행 예정.

Network Type	Layer	Function
User Network (Transport Network)	Service (Data plane)	User data, En/Decryption
	Control & Management	Provisioning, FCAPS, Key access
QKD Network	Quantum	Quantum channel
	Key management	Quantum key distribution
	QKDN Control	Routing control of QKDN
	QKDN Management	FCAPS, Key management, Authentication & Authorization
	QKDN DCN	Management and control network between QKD MCC and QKD nodes

당신의 초능력

kt 5G

peter.park@kt.com