2020년
ICT국제표준 마에스트로
주요이슈 분석서

[양자키분배 네트워크 표준화]

한국정보통신기술협회

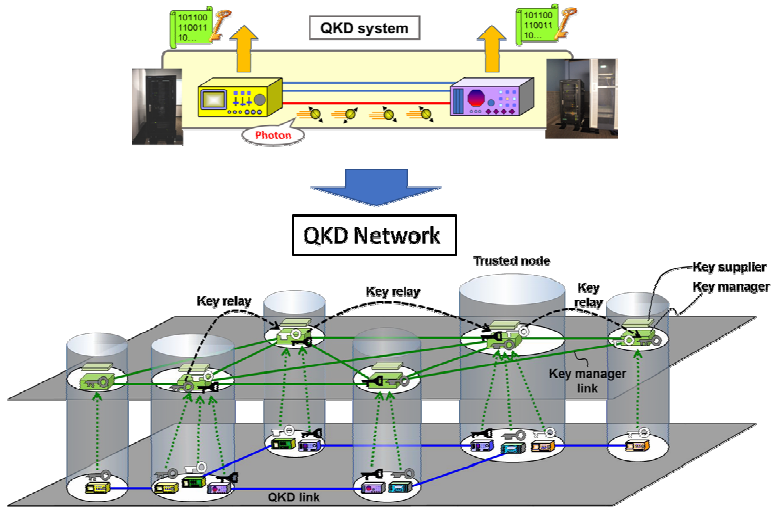
표준 마에스트로 주요이슈 분석서
[양자키분배 네트워크 표준화]

1 개요

1.1 Overall 기술 및 국내외 기술 동향

o 기술 개념

- (양자 정보통신 기술) 양자 역학의 불확실성, 비복원성, 얽히 상태 등을 이용하여 정보를 생성, 전송, 저장, 가공하는 기술로서, 양자 암호 키 분배(QKD)와 큐비트 생성, 가공 등을 포함하는 양자 기반 정보통신 기술
  - 양자통신은 양자암호, 양자전송, 양자 네트워크로, 양자 센서/이미징는 양자측정, 양자센싱, 양자이미징, 양자컴퓨팅은 양자시뮬레이터, 물리양자비트, 논리양자비트, 양자소프트웨어로 각각 세분류함
    *얽힘(Entanglement), 압착(Squeezing), 중첩(Superposition), 결맞음(Coherence)
  - 구체적으로 양자암호 분배 네트워크 기술, 양자암호 제어 및 관리 기술, 양자전송 네트워크, 양자 저장 및 가공 기술을 포함하는 양자 정보통신 기술이 포함됨
  - 기존 QKD 시스템 측면에서 상당히 많은 표준화가 장기간 이루어졌으며, 최근에 이를 진화 발전시켜 QKD 네트워크(QKDN)로 범주를 확장하여 확장성 문제, 장거리 신호 전송의 한계, 안정된 네트워크 운영관리 이슈를 해결하고자 하는 노력이 표준 측면에서도 강조되고 있음



(그림 1) QKD 시스템에서 QKD 네트워크로 기술이 진화 발전함

- (양자 암호통신 및 암호망 표준) 국내에서 개발한 양자 암호키 분배망 기술을 중심으로 ITU-T와 ETSI에 표준과제를 제안하는 등 최근 국내 기업이 국제 표준 활동의 착수를 선도하고 있음

- (양자 정보통신 시험 및 인증 표준) 4차 산업혁명의 구현 기술로 양자 정보통신 기술 개발에 세계 각국이 정부 주도로 박차를 가하고 있음. 상업화와 신시장 창출과 개척을 위해 보안 모듈과 정보통신망 장비의 시험 인증 시스템이 선제되어야 함. 이를 위해 국내 기업 주도로 ITU-T와 ISO에 인증 표준 프로젝트 제안이 진행되고 있음
- 양자 정보통신을 활용한 다양한 응용 분야에 대한 논의가 진행되고 있다. 지능형 네트워크는 양자 정보통신을 통해 개인정보를 보호하고 망동기 및 시각정보 분배 기능을 갖는 광역망 시간 확정형 네트워크를 통해 담당의와의 원격 진료를 제공할 수 있음

o 국내외 정책동향

- (한국) 기획재정부는『양자정보통신 중장기 기술개발사업』을 위해 양자 정보통신 분야의 양자 암호 통신기술을 예비타당성 검토사업으로 지정하고 검토 작업 수행 [2018, 2019]
- (한국) 'ICT R&D 중장기 전략', 절대 보안성을 제공하는 양자 암호통신 유무선 네트워크 및 양자 원천기술, 양자센서 등 실용화를 위해 초신뢰 양자정보통신을 선정 [2017.3]
- (한국) 미래부, 양자정보통신 중장기 추진전략을 발표하였으며, 2015년부터 산학연 컨소시엄을 구성하여 실용화를 대비한 시험통신망 구축 및 안정검증기술 확보를 본격적으로 추진 [2014.12]
- (미국) 양자 기술을 심화하고 연구 인력을 양성하며, 양자산업 육성 추진하기 위한 법안 NIQ 제정. '양자컴퓨팅 연구법' 법률(안)을 추진 중 [2018.12]
- (일본) 문부과학성에서 새로운 가치창출의 핵심 기반기술로서 '광·양자 기술'을 선정하고 "양자과학기술의 새로운 전개 추진방안" 설립 [2017.2]
- (유럽) Quantum Manifesto를 발표하여 유럽이 세계적인 양자정보통신 주도권을 확보하기 위해 양자통신, 양자 시뮬레이션, 양자 센서 및 양자컴퓨터 분야 단기, 중기, 장기 기술 로드맵 수립 [2016.3]
- (중국) 2020년까지 양자 컴퓨터를 개발한다는 목표로 '국립 양자정보과학연구소' 설립 착수 [2017.8]

o 국내 기술동향

- (양자 암호통신 및 암호망 표준) 산학연 협력으로 '양자암호통신망 구축을 통한 신뢰성 검증 기술 및 QKD 고도화를 위한 핵심기술 개발' 통해 기반 기술과 300km 장거리 키 분배 전송을 성공하여 KOREN망에 시험 적용
  - (SKT) 양자 암호분야의 선도기업인 스위스의 IDQ를 인수하여 양자 산업 사업화에 본격적으로 착수 [2018], SKT,우리넷,코위버 등이 OTN과 QKD를 연동하여 NIA의 KOREN 망에 시험 적용 [2018], 안산명화 공업에 5G 기반 스마트 공장에 양자암호를 적용 [2019], 글로벌 마켓 활동으로 도이치텔레콤에 양자암호 PoC [2018], Verizon 네트워크에 양자암호 PoC [2019]

- (KT, KIST) KIST, KT 협력관계로 KT-KIST 양자통신 응용연구센터를 개소 [2017], 10km 거리에서 다자간(1:4) 양자암호통신 시범테스트 구축 [2018]
- (ETRI) 2005년부터 유무선 양자통신연구 기술을 진행하며 무선 양자통신 세계 최초 집적화 핵심 부품 개발 및 무선 양자암호통신 주야간 전송 성공 [2018]

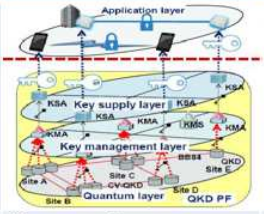
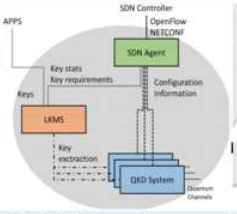
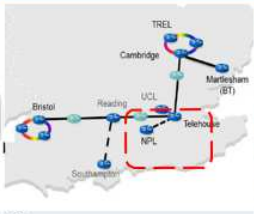
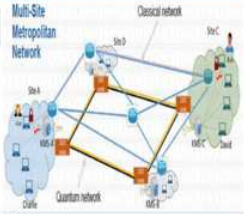
- (양자 정보통신 시험 및 인증 표준) 과기정통부 '양자암호통신망 구축을 통한 신뢰성 검증 기술 및 QKD 고도화를 위한 핵심요소 기술 개발' 과제로 양자암호 키 분배 망에 대한 시험 및 인증 규격 및 절차 개발 중
  - (SKT) 양자 암호분야의 선도기업인 스위스의 IDQ를 인수하여 양자난수생성기(QRNG) 칩 개발 [2018], B2C 5G NW 인증서버 양자난수생성기(QRNG) 적용 [2018]
  - (우리로(주)) InGaAs/InP APD 기반 단일광자검출기 칩 및 모듈 기술 개발 [2018]

o 국외 기술동향

- (양자 암호통신 및 암호망 표준) 전 세계적으로 국가별 연 수천억 이상을 투자하여 양자 암호통신망을 구축해 국가 인프라 구축과 양자통신 분야의 세계 주도권 확보 기술 개발을 위해 노력 중
  - (중국 USTC) 세계 최대 거리인 베이징과 상하이 사이의 2,000km 양자 백본망 구축 완료 [2016], 상하이-베이징 간 QBN으로 은행 망, 통신사망에 양자암호통신 서비스 [2018], 2016년 7월 양자통신 전용 위성 '묵자'호 발사 후 2017년 위성 지상 간 양자키분배 기술 발표, 2018년 2월 위성을 이용한 지상 간의 양자키분배 기술 결과를 발표 [2018]
  - (영국 York 대학) 영국 국가 양자 기술 프로그램의 일환으로 양자통신허브를 구성하여 4개의 작업 패키지를 구성하여 대규모 양자 통신 연구를 수행 중 [2016]
  - (영국 BT) BT 연구소(Adastral Park에 위치)와 26km 떨어진 Ipswich 사이트를 실험실용 광섬유로 연결하여 QKD에 의해 보안성이 확보된 10Gbps 전송 실험 성공 [2017]
  - (퀀텀익스체인지) 월가에 상용서비스망을 통한 양자암호통신 서비스 [2018]
  - (Battelle) 2017년 미국 최초 상업망 내 양자 암호망을 구축하였고, 미국 오하이오~워싱턴 DC를 연결하는 700km 구간의 양자암호통신 시험망 구축 [2018]
  - (워털루 대학) IDQ 센터를 운영 중이며 물리학, 수학, 공학의 실험적 이론적 측면을 이용하여 양자컴퓨팅, 양자통신, 양자 측정 연구기관으로 활동 중[2014]
  - (스페인 텔레포니카) 마드리드에 화웨이에서 개발한 SDN 기반 QKD를 시험 적용 [2018]

- (이탈리아 INRIM) IDQ, 제네바 대학 등과 공동으로 양자암호통신을 위한 Turin-Florence간 650km 광섬유 링크 구축 [2018]

- (양자 정보통신 시험 및 인증 표준) 미래 4차 산업혁명 구현을 위해 양자 정보통신 소자, 양자 컴퓨터 기술을 포함하는 양자 정보통신의 산업화 추진을 위해 규격 개발 및 시험 절차 규정을 위한 노력을 자체적으로 진행 중
  - (스위스 IDQ) SKT가 인수한 스위스의 IDQ에서 양자난수생성기(QRNG) 세계 최초, 소형 칩 개발 [2018]
  - (스위스) 스위스 퀀텀 안정성 시험 수행 [2009-2011]
  - (기타) 각국은 양자암호통신 시험망과 상용망을 구축하여 상용 양자통신 서비스를 진행하면서 자체적으로 시험 절차와 규격을 제정

Function	Tokyo QKD (Japan)	SDN (Spain)	Cambridge Quantum Network (UK)	U. Waterloo (Canada)
				
Key supply	Key supply agent	SD-QKD node	Key management system	Key management system
Key store	Key management agent	SD-QKD node	Key management system	Key management system
ITS key transport	Key management agent + key management server	SDN controller	QKD system + standard IP protocol	QKD network layer
Network controller	Centralized Key management server	Centralized SD-QKD node	Distributed Standard IP protocol + key manager	Distributed QKD network layer
Network configuration	Static	Dynamically reconfigurable	Static/dynamic (depends on the IP routing)	Static
Operation status	Since 2010	Idea (no NW exits)	Partially constructed	Idea (no NW exits)

SD: Software Defined, SDN: Software Defined Network

(그림 2) 해외 QKDN 테스트베트 구축 및 관련 기술개발 현황

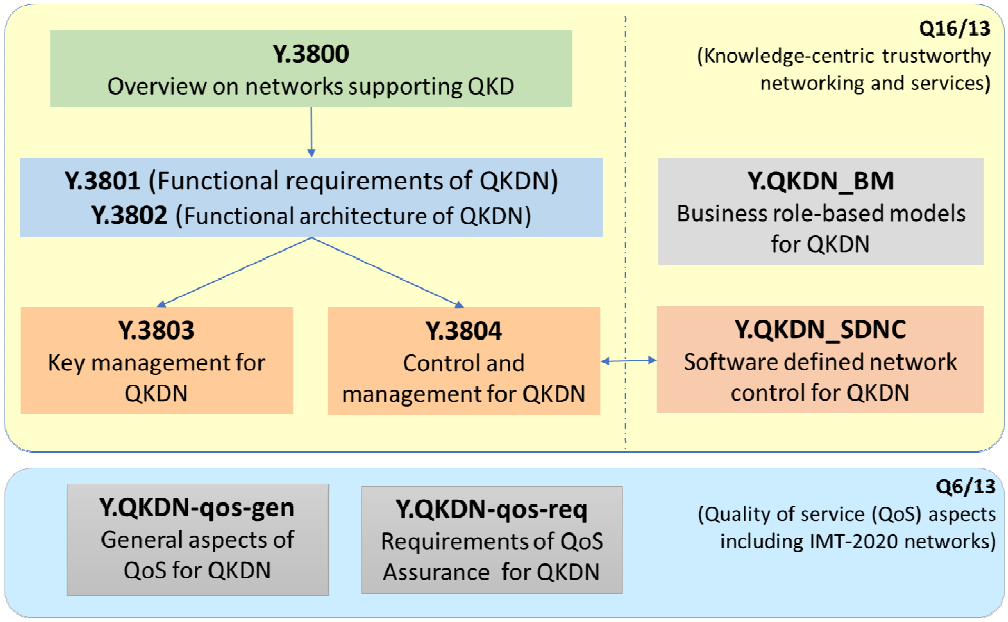
- 상기 기술과 관련하여 ITU-T에서는 다음과 같은 그룹이 관련 표준화 작업을 진행 중

주요 이슈	표준화 그룹	대응 필요성/통찰
QKDN 요구사항, 구조, 키 관리, 운영 관리 기술, SDN 적용방안, 비즈니스 모델 및 서비스 품질	SG13	ITU-T 내에 QKDN 표준화를 선도하고 있고, 네트워크 구조와 이를 실제 구축 가능하게 하기위한 주도적인 역할 필요
QKDN 환경에 적용될 보안 요구사항 및 상세 보안 기술	SG17	보안 기술에 대한 핵심 기술 발굴 및 관련 표준화 필요
네트워크를 위한 양자 정보기술 선행 표준화를 위한 기술 분석	FG-QIT4N	QKDN 개념을 확장하여 전반적인 양자 통신기술 관점에서 새로운 표준화 아이템 발굴 및 선행 표준화 역할 수행

1.2 ITU-T SG13 - 양자키분배 네트워크 표준화 이슈 및 전망

o (개요)

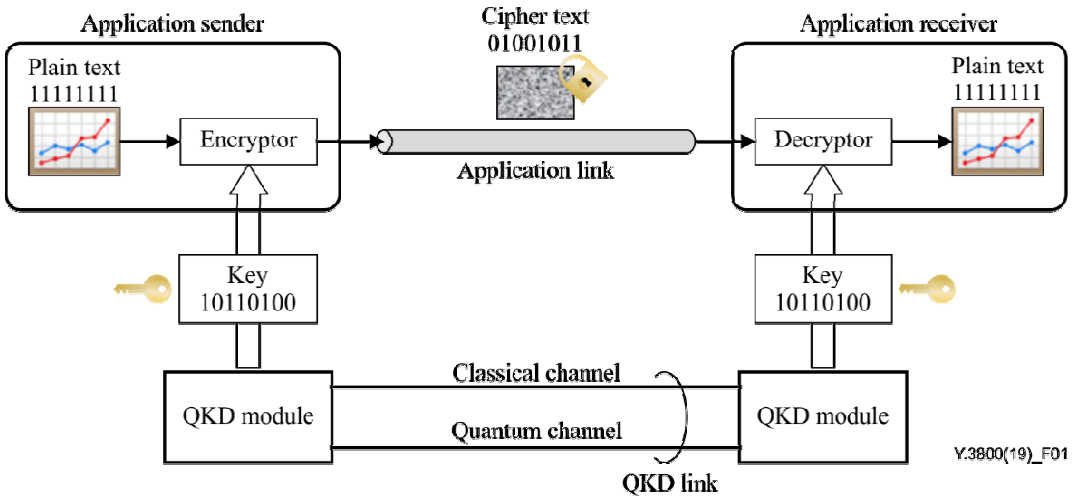
- 2018년 7월 SG13 라포처 그룹 회의에서 KT와 LG유플러스 등 한국 통신사업자 및 국내 양자암호통신 선도 7개 기업 및 기관이 공동제안한 양자암호분배 네트워크 기술에 대한 첫 표준초안이 승인되어 신규 권고안 개발 작업 시작함
- 이후 2019년 3월 짐바브웨 회의에서는 좀 더 구체화된 기능 구조와 키 분배 기술, 운용 관리기술 등에 대한 다수의 표준초안 개발이 신규로 시작됨



(그림 3) ITU-T SG13에서 진행 중인 주요 권고(초)안

o (주요 권고안 내용)

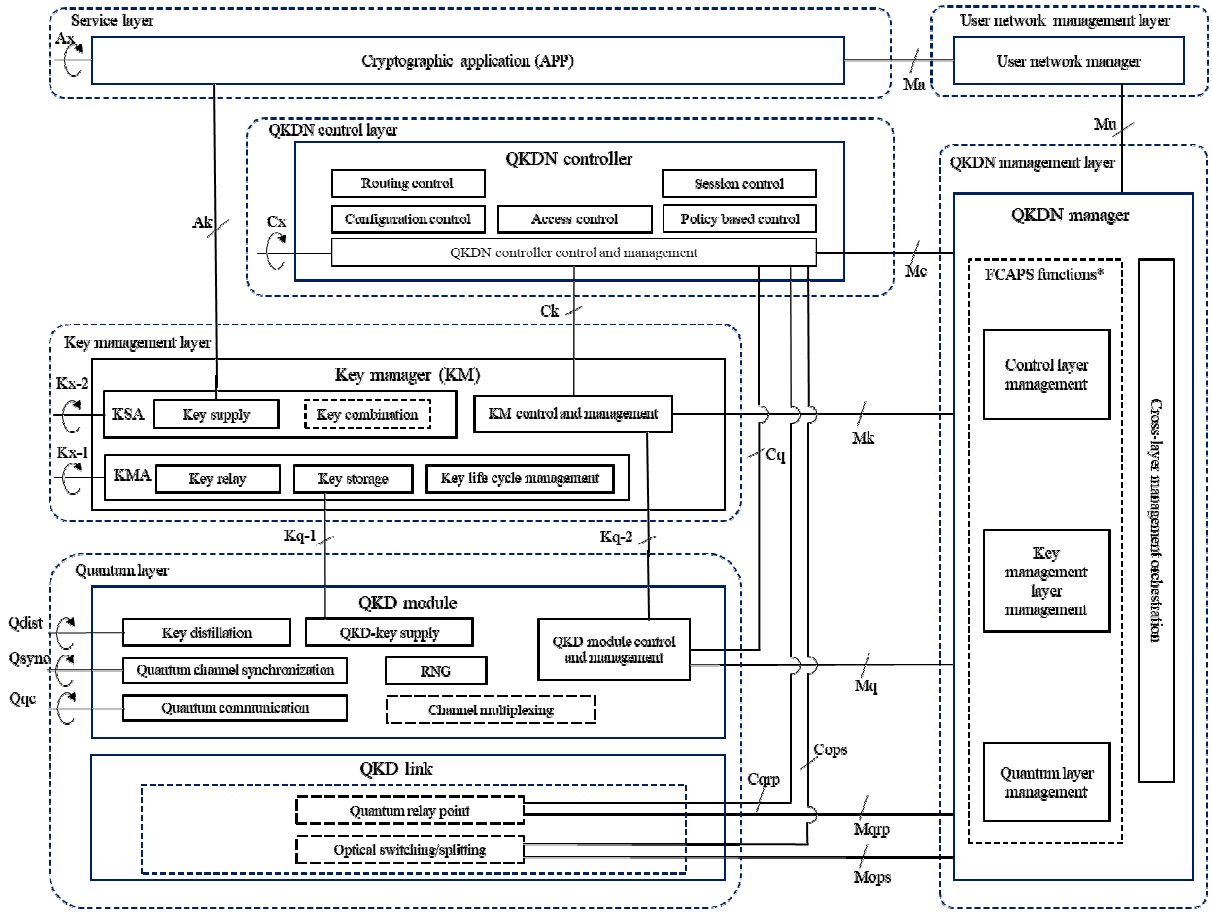
- Y.3800 (04/2020) Overview on networks supporting quantum key distribution, Corrigendum 1



(그림 4) 점대점 애플리케이션 링크 보안을 위한 QKD 사용 구성 예

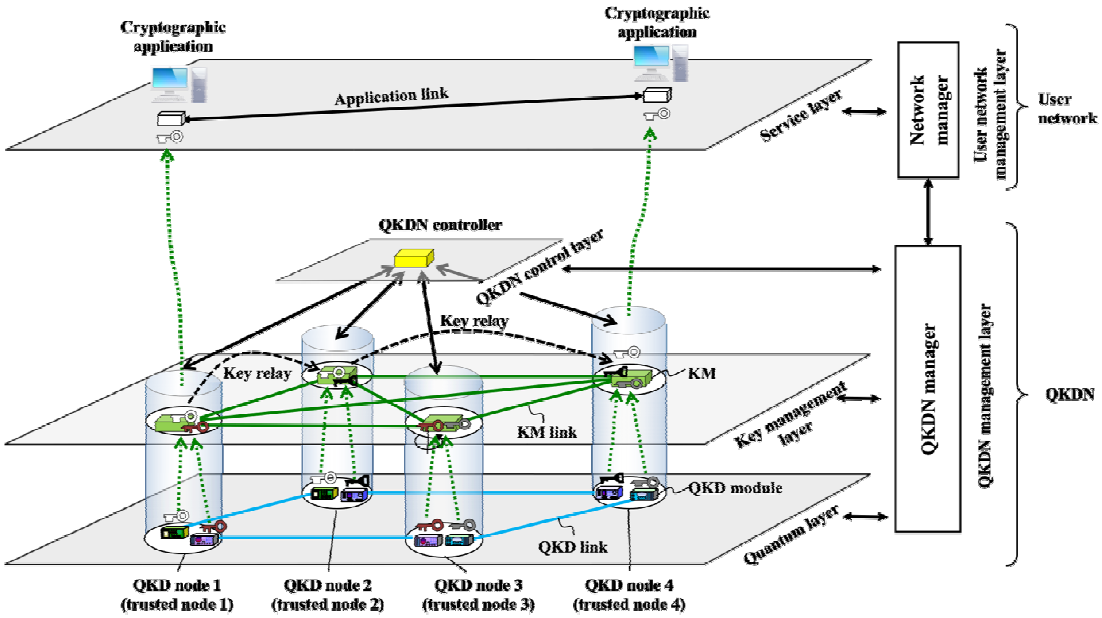
- QKD를 지원하는 네트워크에 대한 개요를 담고 있는 본 권고안은 표준화된 기술 측면에서 QKD 네트워크 (QKDN) 구현을 위한 설계, 배포, 운영 및 유지 관리를 지원하는 것을 목표로 함
- QKD 프로토콜을 사용하면 보안 증명 모델을 지원하는 일부 가정 하에서 제한되지 않은 컴퓨팅 리소스를 사용하는 도청자에 대해서도 보안이 입증될 수 있는 보안 키로 대칭 임의 비트 문자열을 배포할 수 있음
- QKD의 기본 요소는 송신기 (QKD-Tx)와 수신기 (QKD-Rx)이며, 각각을 QKD 모듈이라고 하고 QKD 링크는 잠재적으로 퀀텀 릴레이 포인트의 도움으로 QKD 모듈을 연결함. 키는 QKD 링크를 통해 공유됨. (그림 1)은 점대점 (P-to-P) 애플리케이션 링크를 보호하기 위해 QKD를 적용하는 예를 보여줌

- Y.3801 (04/2020), Functional requirements for quantum key distribution networks
  - QKDN의 맥락에서 양자 계층, 키 관리 계층, QKDN 제어 계층 및 QKDN 관리 계층에 대한 기능적 요구사항을 명세함
- Y.3802, Functional architecture of quantum key distribution networks
  - QKDN의 기능 아키텍처 모델을 정의하는 권고안으로 이를 위해 QKDN의 세부 기능 요소와 참조점, 아키텍처 구성 및 기본 운영 절차를 담고 있음



(그림 5) QKDN 기능 구조 모델

- Y.3803 (승인예정), Quantum key distribution networks – Key management
  - QKD 프로토콜은 무한한 계산 능력을 가진 도청자에게도 안전함이 입증될 수 있는 보안 키로 대칭 랜덤 비트 문자열을 배포하는 수단을 제공함
  - QKDN은 두 개 이상의 QKD 링크와 신뢰할 수 있는 QKD 노드로 구성되며, 여기서 두 QKD 노드 쌍은 QKD 링크 및 키 릴레이를 통해 보안 키를 공유할 수 있음. 이런 키는 사용자 네트워크의 암호화 응용 프로그램에 제공됨
  - QKDN을 구현하고 사용자 네트워크와 적절하게 통합하기 위해 네트워크 기능, 개념적 구조, 계층화된 모델, 기본 기능 및 구성 요소, 사용자 네트워크와의 관계를 포함한 QKD 키와 관련된 핵심 기술을 담고 있음



(그림 6) QKDN에서 키 관리 기능 개요

- Y.3804 (승인예정), Quantum Key Distribution Networks - Control and Management
  - ITU-T Y.3801에 명시된 요구사항에 기반해 QKDN에 의한 안전하고 안정적이며 효율적이며 강력한 운영 및 서비스를 실현하고 전체적으로 QKDN을 관리하고 사용자 네트워크 관리를 지원하기 위한 기능과 절차를 명세함
- Y.QKDN_SDNC, Software Defined Networking Control for Quantum Key Distribution Networks
  - QKDN에서 소프트웨어 정의 네트워킹 (SDN) 기술을 이용한 제어를 위한 요구사항, 참조 모델, 기능 구조, 계층적 SDN 컨트롤러, SDN 제어의 전반적인 운영 절차 및 보안 고려사항을 담고 있음
  - 특히, QKDN에서 SDN 제어의 상세 사례와 기존 QKDN과 SDN기반 QKDN 간의 제어 방법 비교, 제어 가능한 요소 등에 검증 과정이 진행중.
- Y.QKDN_BM, Business role-based models in Quantum Key Distribution Network
  - 일반 QKDN 애플리케이션뿐만 아니라 금융, 의료, 운송 등 다양한 애플리케이션 부문에서 보안 통신을 지원하기 위해 기존 사용자 네트워크를 사용하여 다양한 배포 및 운영 관점에서 QKDN의 비즈니스 역할, 비즈니스 역할 기반 모델 및 서비스 시나리오를 설명함.
  - 이 권고안 초안은 비즈니스 관점에서 QKDN을 적용하고 통신 사업자 관점에서 QKDN을 배포 및 운영하기 위한 지침으로 사용할 수 있음.
- Y.QKDN_frint, Framework for integration of QKDN and secure network infrastructures

  - QKDN을 지원하는 보안 네트워크 인프라의 개요와 QKDN이 다른 네트워크에 향상된 보안을 제공할 수 있는 방법을 제공함
  - 또한 QKDN을 다양한 네트워크(예: 스토리지, 클라우드, 센서, 콘텐츠 등)와 통합 하기위한 높은 수준의 요구사항과 다양한 네트워크에 대한 단계별 시나리오를 제시함
- Y.QKDN_QoS_gen, General Aspects of QoS on the Quantum Key Distribution Network
  - QKDN 구현을 지원하기 위한 설계, 배포, 운영 및 유지 관리를 위해 필요한 양자 키 분배 서비스의 품질 수준을 정의해야 함
  - 따라서 본 권고초안은 상대 매개 변수 및 정의를 포함하여 QKDN 서비스 품질 (QoS) 및 네트워크 성능 (NP)에 대한 설명과 필수로 요구되는 매개 변수 등에 대한 성능 이슈와 분류 체계 등을 제공함
- Y.QKDN_qos_req, Requirements for QoS Assurance of the Quantum Key Distribution Network
  - QKDN의 QoS 보증에 대한 사용 사례 및 관련 높은 수준 및 기능 요구사항을 지정함
- Y.QKDN-qos-arc, Functional architecture of QoS assurance for quantum key distribution networks
  - Y.QKDN-qos-req에 명세한 요구사항과 QKDN의 기능 아키텍처, QKDN의 제어 및 관리를 기반으로 참조 포인트 및 QKDN의 QoS 보증을 위한 기능 특징, 기준점 및 운영 절차를 지정함
- Y.QKDN-qos-ml-req: Requirements of machine learning based QoS Assurance for quantum key distribution networks
  - QKDN은 다양한 QKD 서비스에 대해 최적화된 지원을 제공할 수 있을 것으로 예상되며 KPI (핵심 성과 지표)에는 키 분배를 위한 최적의 대기 시간, 정확도, 처리량 및 가용성이 포함됨
  - QKDN에서 다양한 애플리케이션 시나리오의 네트워크 성능과 다양한 서비스 품질 (QoS) 경험 품질 (QoE) 요구사항을 보장하는 것임
  - 본 권고초안은 QKDN을 위한 기계 학습 기반 QoS 보증의 기능 모델, 기계 학습 기반 QoS 보증의 높은 수준 요구사항 및 기계 학습 기반 QoS 보증의 기능 요구사항을 명세함

ㅇ (해외 대응 현황)

- 일본은 오랫동안 QKD 시험망을 운영해 오는 등 관련분야의 핵심기술을 보유하고 있으나, ETSI 표준 위주의 활동으로 ITU에서의 QKD 네트워킹 표준화에서 방향 전환을 시도하는 중에 있으며, 스위스 역시 상용화 QKD 장비를 생산하는 등 핵심기술 보유하고 있음. 또한 중국도 오랫동안 진행해 온 핵심 기술개발 솔루션을 국제표준에 반영하기 위한 노력을 하고 있음

ㅇ (국내 대응 현황)

- 한국의 통신3사(KT, SKT, LGU+) 모두가 ITU-T SG13 표준개발에 참여개발에 참여하고 있으며 지금까지 쌓은 기술력을 바탕으로 지속적으로 관련 표준화를 주도하고 리더십을 발휘할 수 있는 큰 기회가 되었음

ㅇ (국내 대응 필요성 및 전망)

- 한국은 QKDN을 담당하고 있는 Q16/13에서 라포처를 맡고 있을뿐만 아니라 본 Question이 소속된 트러스트 분야 WP3의 의장까지 맡고 있어 한국 주도로 국제표준을 개발할 수 있는 매우 유리한 상황을 가지고 있으며, 차기 회기에서도 새로운 표준화 항목 발굴 및 표준 특허 개발도 병행해 나가야 할 것임

1.3 ITU-T SG17 – 양자키 분배 네트워크 보안 표준화 이슈 및 전망

ㅇ (개요)

- SG17에서는 2018년 8월부터 양자암호 기술에 대한 표준화 작업을 진행하였으며 초기에 통신망에서 양자키 분배 기술을 위한 보안 프레임워크 및 양자 노이즈 난수 생성기 구조 등의 핵심 표준 개발을 시작함
- 이후 QKDN 측면에서 보안과 특화된 요구사항 및 키 관리와 같은 핵심 암호 기술 등에 대한 표준안 개발을 진행 중

ㅇ (주요 권고(초)안 내용)

- X.1702, Quantum noise randum number generator architecture
  - 암호화 알고리즘에서 핵심 기능으로 요구되는 난수생성기와 관련하여 양자기술 기반의 난수 생성기의 구조와 원리를 본 표준에 정의
- TR.sec-qkd, Security considerations for quantum key distribution network
  - QKDN 소개, QKD 시스템과 애플리케이션 (암호화 애플리케이션) 통신 엔티티 간의 통신에서 보안 고려 사항, QKD 시스템과 관리 및 모니터링 시스템 간의 통신에 대한 보안 고려 사항, 표준화 이슈 및 향후 작업 제안
- X.sec_QKDN_tn, Security requirements and designs for quantum key distribution networks - trusted node
  - QKDN에서 신뢰할 수 있는 노드를 안전하게 구현하고 운영하기 위한 가이드라인을 제시하는 것을 목표로 이들 노드의 보안 위협, 보안 요구 사항 및 이를 달성하기 위한 구현 예를 제시함
- Security requirements and designs for quantum key distribution networks–key management
  - QKDN의 키 관리에 대한 보안 위협, 키 관리를 위한 보안 요구사항 및 보안 요구사항을 충족하기위한 키 관리의 보안 조치를 명세하고 이를 바탕으로 QKDN의 키 관리의 설계, 구현 및 운영을 지원
- X.1714 (former: X.cf_QKDN), Key combination and confidential key supply

for quantum key distribution networks

- QKDN에서 암호화 응용 프로그램으로의 키 조합 및 키 공급 모두에 대한 보안 요구사항을 지정하는 것을 목표로 QKDN을 통해 교환된 키와 다른 키 교환 방법을 통해 교환 된 키 조합의 보안 및 QKDN에서 암호화 애플리케이션으로의 키 공급 보안을 포함

- X.1710, Security framework for quantum key distribution networks
  - 보안 위협에 대처하기위한 요구사항 및 조치를 포함하여 QKDN에 대한 프레임워크를 제시하기 위해 단순화된 QKDN 구조 및 관련 보안 위협뿐만 아니라 보안 요구사항 및 해당 보안 조치에 대한 가이드라인을 포함
- X.sec_QKDN_intrq, Security requirements for integration of QKDN and secure network infrastructures
  - 다양한 사용자 네트워크 (예: 스토리지, 클라우드, 센서, 콘텐츠 등)에서 서비스 계층과 QKDN의 통합을 위한 보안 요구사항을 명세하고, QKDN을 기존 및 새로운 보안 네트워크 인프라와 통합하기위한 프레임워크를 제시함

ㅇ (해외 대응 현황)

- SG13과 마찬가지로 일본, 중국뿐만 아니라 유럽 주요국에서 QKDN 보안 측면 표준개발에 적극적으로 참여하고 있음
- 중국은 FG-DPM 활동에 매우 적극적이어서 초기부터 데이터 연동 및 블록체인 기술을 적용한 데이터 공유 등과 관련된 표준 개발에 매우 적극적이다. 또한 데이터 트러스트 관련 문서개발에도 함께 참여하였음
- UAE는 데이터 경제 측면에서 데이터를 가치화하고, 상용화하기 위한 프레임워크 개발을 주도하였음

ㅇ (국내 대응 현황)

- SKT 및 자회사인 IDQ 등이 적극적으로 참여하여 에디터십을 가지고 관련 권고안 개발을 주도하고 있으며, 타 통신사업자 등도 함께 표준 개발에 참여중

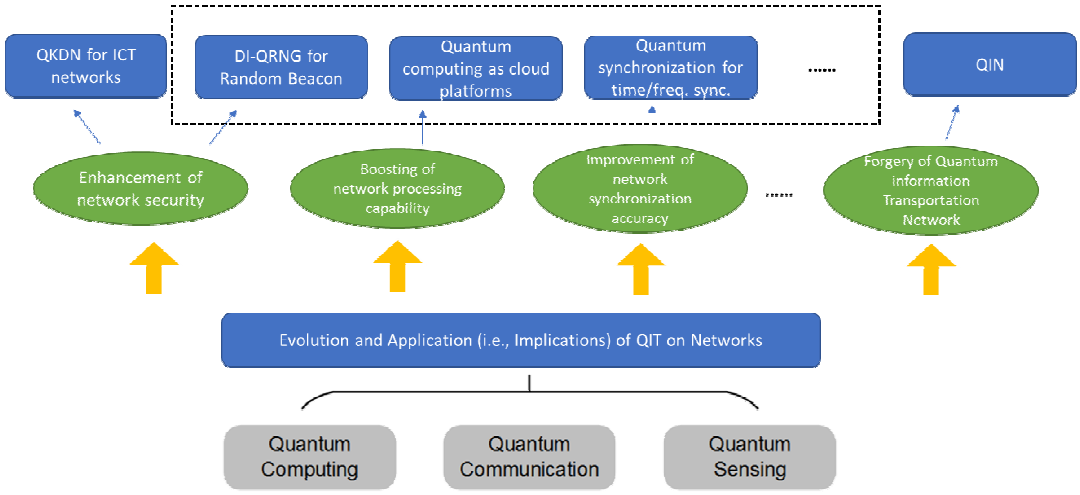
ㅇ (국내 대응 필요성 및 전망)

- SG17은 한국이 SG 의장직을 수임하고 있으며, QKDN 보안기술을 담당하고 있는 Q4/17 또한 한국이 라포처 및 부라포처를 맡아 표준 개발을 전담하고 있음. 이러한 리더십을 바탕으로 관련 국제 표준안 개발이 순차적으로 이루어질 수 있도록 노력할 예정임

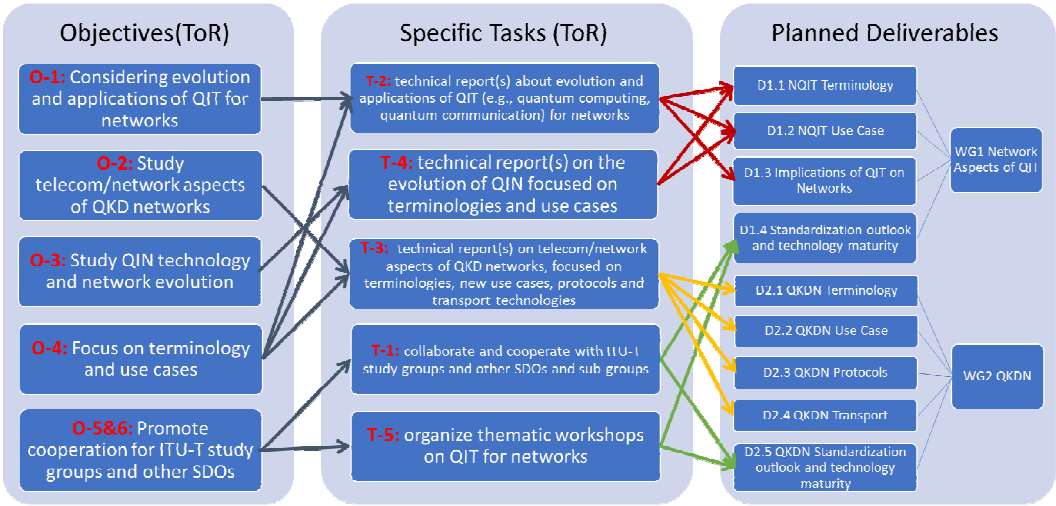
1.4 ITU-T FG-QIT4N 네트워크를위한 양자정보기술 표준화 이슈 및 전망

ㅇ (개요)

- 양자 정보 기술 (QIT)은 양자 역학의 원리를 활용하여 정보 처리 능력을 향상시키는 신흥 기술로 2차 양자 혁명의 붐을 일으켰으며 ICT 네트워크에 큰 영향을 미칠 것임



(그림 7) 네트워크를위한 양자정보기술의 핵심요소



(그림 8) FG-QIT4N 주요 목표, 임무 및 예상 결과물

- 네트워크를위한 양자 정보 기술에 대한 ITU-T 포커스 그룹 (FG-QIT4N)은 네트워크를 위한 QIT의 사전 표준화 측면을 위한 협업 플랫폼을 제공하기 위해 2019년 9월 TSAG 회의에서 다음과 같은 주요 목표로 설립되었음
  - 네트워크를위한 QIT의 진화 및 응용 연구
  - 네트워크를위한 QIT의 용어 및 사용 사례에 중점을 둠
  - ITU-T 연구 그룹에서 QIN 관련 표준화 작업을 효과적으로 지원하기위해 필요한 기술적 배경 정보 및 협력 조건을 제공
  - ITU-T SG 및 기타 SDO와 개방형 협력 플랫폼을 제공

o (주요 Deliverable 내용)

- D1.1 QIT4N terminology part 1: Network aspects of quantum information technology
  - QIN을위한 빌딩 블록으로 QIN에 필요한 기술로 애플리케이션 중심 네트워크 요구사항과 기존 네트워크의 이점을 살펴보기 위해 양자정보기술에

대한 용어 수집, 분석 및 분류에 대한 상세 내용 포함

- D1.2 Technical Report on QIT4N use case part 1: Network aspects of Quantum Information Technology
  - QIN(Quantum Information Network) 기반 QIT 사용 사례, 클래식 네트워크에 유용한 QIT 사용 사례 및 네트워크가 QIT 애플리케이션에서 본질적인 역할을 하는 QIT 사용 사례를 분석함
- D1.3 Technical Report on the Implications of Quantum Information Technology for Networks
  - QIN을위한 빌딩 블록으로 낮은 수준의 필수 구성 요소에서 높은 수준의 시스템에 이르기까지 양자 정보 네트워크의 근본적인 측면을 제공하는 QIN에 필요한 기술과 애플리케이션 기반 네트워크 요구사항을 분석함
- D1.4 Standardization outlook and technology maturity part 1: Network aspects of QIT
  - 네트워크용 QIT 표준화 환경의 분석, 네트워크용 QIT 표준의 개발 및 채택에 대한 전망과 장벽 및 네트워크에 대한 QIT의 기술 성숙도와 표준화 준비 상태를 평가하기 위한 방법론을 검토함
- D2.1 QIT4N Terminology Part 2: Quantum Key Distribution Networks
  - QKDN 용어 표준화 활동에 참여하는 SDO, 학계 및 산업 컨소시엄 등에서 정의해 둔 용어 정의를 제시하고 비교 분석함
- D2.2 QIT4N use case part 2: Quantum Key Distribution Network
  - QKDN의 사용 사례를 연구를 위해 QKDN이 가져 오는 경쟁 우위, 수직 및 수평 도메인의 QKDN 사용 사례 및 QKDN 채택의 장벽 등을 분석함
- D2.3 Quantum key distribution network (QKDN) protocols part 1: Quantum layer
  - QKDN의 양자 계층에 있는 프로토콜을 관련 다양한 유형의 QKD 프로토콜, 워크 플로우, 프로토콜 기능, 매개 변수, 상용화 상태, 보안 증명, 향후 네트워크에 통합될 가능성 등에 대한 기술을 분석함
- D2.3 Quantum key distribution network (QKDN) protocols part 2: Key management layer, QKDN control layer, and QKDN management layer
  - QKDN의 키 관리 계층, QKDN 제어 계층 및 QKDN 관리 계층과 관련된 통신 프로토콜을 분석함
- D2.4 QKDN transport technologies
  - 전송 시스템 구성 요소, 기술 솔루션, 양자 및 고전 신호 전송 요구사항 등과 같은 QKDN 전송 기술에 분석을 진행
- D2.5 QIT4N standardization outlook and technology maturity part 2: quantum key distribution network
  - QKDN 표준화 전망과 기술 성숙도를 위해 QKDN 기술 및 산업 개발 개

요, 기술 성숙도 평가, 표준화 환경 및 격차 분석 및 전망을 포함

ㅇ (해외 대응 현황)

- 포커스 그룹 신설 시에 상당히 많은 회원국으로부터 관심을 받았으나 현재는 거의 대부분의 Deliverables 개발을 중국에서 맡아서 하고 있는 중이며, 다른 회원국은 대부분 진행 사항을 모니터링하는 수준에 머물러 있음

ㅇ (국내 대응 현황)

- 국내 KT, SKT에서 부의장으로 참여하면서 적극적인 표준화 활동을 예상했지만 기존 SG에서 진행 중인 표준화에 치중하면서 현재 포커스 그룹 활동에는 큰 역할을 하고 있지는 않음

ㅇ (국내 대응 필요성 및 전망)

- FG-QIT4N 활동이 종료되면 결과물이 해당 주제를 담당하는 SG으로 전달됨에 따라 향후 이를 표준 권고안 형태로 만드는 작업이 잘 진행될 수 있도록 하고, QIT4N에서 다루고 있지 않은 주제에 대한 표준화 아이템 발굴 노력 필요

1.5 기타 표준화 그룹 양자키분배 네트워크 표준화 이슈 및 전망

ㅇ (ITU-T SG15)

- ITU-T SG13에서 첫 QKDN 권고안 개발 작업을 시작한 후 SG15를 포함 관련 SG에 관련 표준 착수를 통보하는 liaison을 송부하였고 Q12/15에서 검토됨
- SG15는 광기술 기반의 데이터전송 표준을 리딩하는 그룹으로 제안된 QKDN 기술이 광전송기술과 어떠한 연관성을 가지고 있는지 논의
  - 양자키는 기존의 전송 기술에서 사용하는 전통적인 광신호 전달 방법이 아니기 때문에 SG15의 표준업무와 직접적인 연관성이 없다는 의견이 있었음
- SG15에서 표준화하고 있는 전송 시스템은 데이터 전송을 위한 시스템으로 양자키 전송을 위해서 사용되기 어렵고 양자키를 전달하기 위한 물리적인 특성(예를 들어, 광 특징, 등)에 대한 추가적인 정보 제공이 요구됨

ㅇ (ETSI QKD ISG)

- QKD 모듈 보안 규격 표준 제정으로 양자 키 분배망의 시험 절차 및 인증 규격을 표준화. 이후 표준과제를 통해 보안의 보안성 증명 등을 추진
- 주요 표준 내용
  - ETSI GS QKD 003 v1.1.1 (2010-12) Quantum Key Distribution (QKD); Components and Internal Interfaces (TTAE.ET GS QKD 003 (2017년 6월 28일) 양자키 분배: 구성 요소 및 내부 인터페이스): 이 표준에서는 정의하는 양자 키 분배 표준의 범위를 QKD 구성 요소 및 내부 인터페이스에 한하여 규정
  - ETSI GS QKD 004 v1.1.1 (2010-12) Quantum Key Distribution: Application Interface (TTAE.ET-GS QKD 004 (2017년 12월 13일) 양자키

분배망: 응용 인터페이스): 이 표준에서 정의하는 양자 키 분배 표준의 범위를 응용 인터페이스에 대한 규정

- ETSI GS QKD 008 v1.1.1 (2010-12) Quantum Key Distribution (QKD); Module Security Specification (TTAE.ET GS QKD 008 (2018년 12월 19일) 양자 키 분배 (QKD): QKD 모듈 보안 규격): 이 표준에서 정의하는 양자 키 분배 표준의 범위를 QKD 시스템의 모듈에 대한 보안 요구사항 및 보안 규격
- ETSI GS QKD 011 v1.1.1 (2016-05) Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems (TTAE.ET-GS QKD 011 (2018년 6월 27일) 양자 키 분배(QKD); 구성 요소 특성화: QKD 시스템의 광학 구성 요소 특성화): 이 표준은 양자 정보통신 분야의 양자 키 분배 (QKD) 시스템의 구성 요소 특성화에 대한 표준으로서 QKD 시스템의 구성 요소인 광소자의 특성과 특성 파라미터의 측정 방법 및 절차를 규정

ㅇ (IETF/IRTF – 양자 인터넷 연구 그룹 (QIRG))

- 전반적으로 QIRG의 목표는 양자 네트워크를 설계하고 구축하는 방법에 대한 질문들에 대한 해결책을 찾는 것을 목표로 함
  - 라우팅: 양자 네트워크에서 최적의 경로를 찾는 것은 특정 충실도 임계값을 달성해야 하고 양자 메모리의 일관성 시간이 낮기 때문에 이를 위한 적합한 라우팅 체계가 필요
  - 리소스 할당: 모든 네트워크에는 한정된 리소스 풀이 있으며, 양자 네트워크는 양자 메모리의 일관성 시간과 같은 새로운 리소스 고려가 필요
  - 연결 설정: 양자 네트워크는 패킷 대신 얽힌 상태를 전달하므로 연결 의미가 다를 수 있는 특징이 있음
  - 상호 운용성: 서로 다른 하드웨어를 기반으로하고 서로 다른 프로토콜을 사용하는 서로 다른 네트워크가 현재 설계 및 구축되고 있음
  - 보안: 양자 네트워크는 애플리케이션의 보안을 강화함에 따라 네트워크 자체의 보안 문제도 해결해야 함
  - API 디자인: 클래식 소켓은 비트 개념을 중심으로 구축되는데 충실도 및 양자 메모리의 낮은 일관성 시간과 같은 새로운 고려 사항에 따라 얽힌 상태에 대한 API에 대한 검토 필요
  - 양자 인터넷을위한 애플리케이션: 양자 통신의 저수준 추상 기능을 퀀텀 인터넷에서 제공하는 서비스로 전환하는 방법을 분석하여 양자 서비스를 완전한 정보 시스템에 통합
  - 네트워크 코딩과 같은 다자간 상태 및 다자간 전송: 단순하고 독립적인 지점 간 전송이 아니라 더 복잡한 상태를 만들고 사용 가능토록 해야 함
- Applications and Use Cases for the Quantum Internet

<draft-irtf-qirg-quantum-internet-use-cases-03> 2020.09.

- 퀀텀 인터넷에서 사용될 것으로 예상되는 일부 애플리케이션의 개요를 제공한 다음 다양한 분류 체계를 사용하여 분류, 퀀텀 인터넷에 대한 몇 가지 일반적인 요구사항 설명

- Architectural Principles for a Quantum Internet < draft-irtf-qirg-principles-05> 2020.09.
  - 양자 얽힘의 근본적으로 새로운 특성을 고려하여 양자 네트워크 스택을 처음부터 구축해야 함을 주장하고 이를 지원하기 위한 양자 인터넷에 대한 몇 가지 기본 아키텍처 원리를 소개

ㅇ (NIST, ANSI)

- 미국 보안표준 진행하는 NIST, ANSI에서는 기존 고전 암호키를 통한 암호 알고리즘과 인증 알고리즘을 개발 중으로 양자 정보통신 표준분야에서는 양자 키 적용과 암호화 연동을 위해 기존의 ANSI, IETF 표준 알고리즘과의 호환을 염두에 두고 표준 진행 중 [2018]
- 양자정보통신 상업망 구축과 사업화를 위한 보안시스템 인증 기준을 개발할 계획 [2020]

ㅇ (기타 표준화 기구)

- CSA-QSS (Cloud Security Alliance-Quantum Safe Security Working Group): QKD 및 PQC (post-quantum cryptography)를 통해 데이터를 보호하기 위한 양자 안전 방법으로 키 생성 및 전송 방법에 대한 표준화 진행
- IEEE P1913: 소프트웨어 정의 양자 통신에 대한 표준화 진행
- JTC1 SC27: 양자 암호통신 관련 SC 표준을 추진할 예정 [2022]

2 국제표준화 영향력 확대 방향 및 전략

2.1 국제표준화에서 한국의 취약점

ㅇ 산학연 연계 국가주도 표준화 필요

- ITU-T SG13에서 시작된 본 표준안 개발은 전통적으로 네트워크 기술 개발을 전담해 온 그룹 측면에서 양자 암호통신을 위한 네트워크 구조 및 기능, 양자 암호 네트워크 전송장비간 인터페이스, 서비스 절차 등의 상세내용을 국제 표준으로 채택될 수 있도록 노력함
- 한국 통신사업자들이 주도적으로 참여하고, 상용통신망에서 양자암호통신을 구축하는 방법과 해킹 시도에 대응하는 시나리오에 대응하는 시나라오를 도출하고, 관련 기술 상용화를 위한 발판을 마련했다는 측면에서 의미가 큼

ㅇ 관련 표준 그룹간 협력 및 경륜 있는 전문가 필요

- 일반적으로 ITU-T 표준화 활동에 있어 공통적으로 제기되는 다음과 같은 문제점을 극복할 수 있는 관련 표준 그룹간 협력 및 경륜 있는 전문가가 요구됨
  - 중복성 문제: 신규 연구항목에 대한 검토 때마다 항상 등장하는 것이 ITU-T내 다른 SG 뿐만 아니라 다른 SDO간의 중복성 문제이고, 여기에 대한 논의에 대부분을 시간을 소비해 버린다. 각 SG의 큰 항목 기술요소는 기본적으로 광범위한 기술 영역을 포함하고 있어서 좀 더 세분화하여 여러 측면에서 기술의 다양성을 바라볼 수 있어야 함
  - 전문성 문제: QKDN 경우 네트워크 기술과 보안 기술이 함께 접목되어 있는 분야이어서 사안에 따라 상당한 기술적 논란이 되는 경우가 많다. 이런 분양의 표준안 개발에는 실제 통신망을 운용해 보고, 장비 개발 및 상용화를 해 본 전문 인력이 표준안 개발에 적극 참여할 수 있도록 해야함
  - 협력 문제: 각 Question 별로 Terms of Reference(작업범위)를 만들어 두었으나 이들 Question들 간의 협력이 힘든 경우가 많다. QKDN 관련해서는 SG13과 SG17간의 협력을 위하여 CQ(Co-located Quantum) 미팅을 신설하였으며 이슈가 있을 때마다 조인트 회의를 통해 문제점을 해결해 나갈 수 있도록 노력하고 있음
  - 목표 문제: SG에서 특별히 지향하는 바가 정확해야 하는데, 따로는 목표하는 바가 없어서 조금이라도 유사주제를 다루는 그룹에서 엄청나게 많은 liaison 문서를 보내오고 이를 검토하고 있는데, 실효성에 의문이 들고 오히려 짐이 되고 있는 상황인데, 이 보다는 각 SG에서 목표로 하는 분야를 좀 더 세분화하여 정할 필요가 있음
- 한국은 이미 15년 이상 경륜 있는 표준 전문가를 일부 확보한 상태이지만, 여전히 국제표준화를 추진하는데 있어 상기와 같은 애로사항이 있는 것이 사실이다. 이를 극복하기 위해 더 많은 고급 표준화 전문가 풀(Pool) 육성이 필요
- 표준화 회의에서는 기술에 대한 이해뿐만 아니라 유창한 영어 실력까지 겸비하고 국제 전문가들간의 교류 및 인맥을 좀 더 넓힐 수 있어야 함

2.2 취약점 개선을 위한 전략(접근방법 등)

ㅇ 관련 그룹간 표준화 협력을 위한 리더십 확보

- 2021년부터 시작되는 ITU-T 차기 회기에는 좀 더 효율적으로 원하는 방향의 표준안 개발이 가능하도록 하기 위해서는 다음과 같은 전략이 필요
  - SG이 지향하는 비전 제시: 각 SG에서 다루고 있는 주요 표준화 방향을 바탕으로 표준이 목표하는 방향을 먼저 제시하고, 여기에 맞춤형 기고가 이루어질 수 있도록 해야 한다. 최근에 QKDN에 관한 5건의 핵심 권고안 개발을 마무리한 SG13의 경우 이를 바탕으로 추가 권고안 개발 작업이 순조롭게 이루어질 수 있도록 SG 차원에서의 워크숍 등을 개최하여 신규 연구 항목에 대한 논의와 향후 표준화 방향에 대한 안을 만들고 이를 통해 좀 더 효율적이고 체계화된 표준화가 진행될 수 있도록 함
  - 향후 표준화 방향에 대한 로드맵이 필요: 워크프로그램을 통해 발간된 권고안이나 진행 중인 권고안에 대한 상세 정보를 관리하고, 향후 표준화 핵심 연구항목에 대한 큰 그림을 담은 로드맵을 제시할 필요가 있음. 이를 이용하여 양자 통신기술 분야 신규 연구항목에 대한 논의 시에는 각 SG에서 제시하는 표준화 로드맵을 바탕으로 표준개발의 당위성을 쉽게 설명하고 계획적인 표준안 개발이 이루어질 수 있도록 해야 함
  - CQ 미팅의 적극적 활용: 관련 Question 간의 협력이 매우 중요한 토픽 중의 하나가 QKDN 기술이다. 앞서 언급했듯이 통신망 기술뿐만 아니라 보안 기술을 함께 표준안에 담기 위하여 SG13 입장에서는 보안 기술에 대한 전문성이 추가로 요구되고, SG17 입장에서는 통신망 기술에 대한 전문성이 필요함에 따라 차기 회기에도 CQ 미팅을 적극 활용하여 두 그룹 간 적극적인 협력을 통해 관련 표준안 개발이 이루어질 수 있도록 해야 함
  - 표준화 전략 마련: 앞서 언급한 지금까지 나타난 여러 가지 애로사항을 해결하기 위하여서는 무엇보다도 체계적인 전략을 수립하고, 이를 회의 참석자와 의견을 수렴해가는 과정이 필요하다. 각 SG Management Team에 전문가가 필요하고, 이들이 회의 참석자들에게 표준개발에 대한 정확한 가이드라인을 제공해 주어야 하며, 보안 및 빅데이터 등의 관련 SG과의 중복성 이슈에 전략을 가지고 적절한 대응을 해 나가야 함

2.3 우리나라이 리더쉽 확대 방안

ㅇ (ITU-T SG13 전체 의장단 현황)

개발기구	의장단 현황	이름/소속	특이사항
ITU-T SG13	SG13 의장	Leo LEHMANN/스위스	
	SG13 부의장	Mohammed AL TAMIMI/중국 CITC	WP3 부의장
	SG13 부의장	Rim BELHASSINE-CHERIF/튀니스 텔레콤	WP3 부의장
	SG13 부의장	Ahmed EL-RAGHY/이집트 TRA	WP2 부의장
	SG13 부의장	Yoshinori GOTO/일본 NTT	WP2 의장
	SG13 부의장	김형수/한국 KT	WP1 의장
	SG13 부의장	Scott MANSFIELD/Ericsson Canda	
	SG13 부의장	Juan Carlos MINUTO/아르헨티나	WP2 부의장
	SG13 부의장	Brice MURARA/루완다	WP1 부의장
	SG13 부의장	Fidelis ONAH/나이지리아	WP2 의장
	SG13 부의장	Heyuan XU/중국 MIIT	WP3 의장
	SG13/WP1 의장	Luca PESANDO/이탈리아 텔레콤	
	SG13/WP1 부의장	Alojz HUDOBIVNIK/슬로베니아 Iskratel	
	SG13/WP1 부의장	Lu LU/차이나 모바일	
	SG13/WP3 의장	이규명/한국 KAIST	

- SG13에 있는 총 13개 Question 중에 총 6개 Question의 라포처를 한국 전문가가 맡고 있음
  - Q1/13: 서비스 분야, 정희창 (동의대), Q6/13: Qos 분야, 최태상 (ETRI), Q16/13: 신뢰 통신망 분야, 이규명 (KAIST), Q17/13: 클라우드 컴퓨팅 분야, 이강찬 (ETRI), Q20/13: 5G 네트워크 요구사항 및 구조, 고남석 (ETRI), Q23/13: FMC(Fixed Mobile Convergence) 분야 김정윤 (ETRI)

ㅇ (ITU-T SG17 전체 의장단 현황)

개발기구	의장단 현황	이름/소속	특이사항
ITU-T SG17	SG17 의장	염흥렬/한국 순천향대학교	
	SG17 부의장	Vasiliy DOLMATOV/러시아	WP1 부의장
	SG17 부의장	Gökhan EVREN/터키	WP1 부의장
	SG17 부의장	Juan GONZALEZ/미국	WP2 부의장
	SG17 부의장	Muataz Elsadig ISHAG/수단	
	SG17 부의장	Zhaoji LIN/중국 ZTE	WP4 의장
	SG17 부의장	Eric Anicet MBATHAS/중앙아프리리카공화국	
	SG17 부의장	Yutaka MIYAKE/일본 KDDI	WP1 의장
	SG17 부의장	Lia MOLINARI/아르헨티나	
	SG17 부의장	Wala TURKI LATROUS/튀니지아	
	SG17/WP2 의장	Koji NAKAO/일본 NICT	
	SG17/WP3 의장	Arnaud TADDEI/스위스	
	SG17/WP3 부의장	Xiaoyuan BAI/중국 Alibaba	
	SG17/WP4 부의장	나재훈/한국 ETRI	

- SG17에 있는 총 14개 Question 중에 총 6개 Question의 라포처를 한국 전문가가 맡고 있음

ㅇ (ITU-T FG-QIT4N 전체 의장단 현황)

개발기구	의장단 현황	이름/소속	특이사항
ITU-T FG-QIT4N	FG-QIT4N 의장	Alexey Borodin/러시아	
	FG-QIT4N 의장	James Nagel/미국	
	FG-QIT4N 의장	Qiang Zhang/중국, USTC	
	FG-QIT4N 부의장	Fahad Alduraibi/사우디아라비아	
	FG-QIT4N 부의장	Helmut Griesser/독일	
	FG-QIT4N 부의장	Kaoru Kenyoshi/일본	
	FG-QIT4N 부의장	김형수/한국, KT	
	FG-QIT4N 부의장	Junsen Lai/중국, QuantumCTek	
	FG-QIT4N 부의장	Jiajun Ma/중국, CAICT	
	FG-QIT4N 부의장	Momtchil Peev/독일 Huawei	
	FG-QIT4N 부의장	심동희/한국 SKT	

ㅇ (국제표준화 진출 및 확대 필요성 및 전망)

- 한국 주도 연구개발 결과가 국제 표준으로 반영되고, 이를 연계하여 표준특허도 발굴할 수 있도록 연계 추진이 바람직하다.
- 선행표준 개발을 위해 국제 표준화 기구에서 포커스그룹 및 표준화 로드맵 개발 등에 참여도 중요하다.

ㅇ (국제표준화 진출 및 확대 전략)

- 의장단 활동 강화: 표준화 회의에서 의장단의 역할이 점차 중요해지고 있으므로, 의장단 활동을 통해 표준화 주도권 확보에 유리할 수 있도록 해야하며, 한국이 강점을 가질 수 있는 분야 신규 의장단 진출에 적극적이어야 함
- 전문가 인프라 확대: 표준전문가 육성을 위한 관련 교육 및 멘토링 기회 확대를 통해 신규로 양자기술 국제표준화에 참여할 수 있도록 장려
- 정부의 지속적 지원: 통신사업자와 통신 장비업체 중심으로 국산기술의 상용화와 이를 국제표준에 반영하려는 노력이 지속적으로 요구되며, 기술에 대한 검증 또한 중요하기 때문에 시범사업 등을 장려할 필요가 있음.
- 국민행복 안전보장 측면: 양자 암호기술의 가장 핵심은 보안임에 따라 금융, 국방, 의료 등 생활안전, 의료서비스 향상, 국민 안전 및 편의가 향상된 서비스에 높은 수준의 보안이 적용될 수 있는 표준개발을 위해 노력 필요

3. 시사점 및 결언

ㅇ (시사점)

- QKDN에서 시작된 표준화가 향후에 양자정보통신 전반적인 분야로 확대되면서 암호통신뿐만 아니라 양자 컴퓨팅, 양자 센싱 등의 신기술은 4차산업혁명 시대에 신사업을 창출하는데 있어 핵심이 될 것이며, 핵심 기술개발을 통한 비즈니스와 일자리 창출에 큰 기여를 할 것으로 예상되며, 이에 따른 선제적인 국제표준화 아이템 발굴 및 산학연 협력을 통한 국제표준 기반 기술개발 및 적용에 앞장서야 할 것임
- 표준의 활용 측면에서 기존 네트워크 인프라 및 서비스에서 보안이 중요한 응용 분야부터 시범적으로 서비스를 적용할 수 있도록 통신사업자뿐만 아니라 관련 장비 및 암호기술, 각종 네트워킹 솔루션 업체 등이 상호 운용성이 보장될 수 있는 기술개발과 개방형 산업생태계 활성화에 기여해야 할 것임

ㅇ (정책적 방향 제시)

- 장비제조사 중심 All-in-one 형태의 유럽표준기술 활용 시 기술종속이 불가피하지만 최근에 암호기술 이외의 네트워크 측면의 통신장비, 네트워크 운용관리 소프트웨어 등으로 국내 ICT 생태가 성숙 되어감에 따라서 국내기술 주도로 해외 기술의 종속성을 해결할 수 있고, 시범사업 발굴, 산학연 연계 및 전문가 활용을 통한 국제표준화의 주도권을 확보, 표준 특허 개발과도 연계 필요

ㅇ (결언)

- Q16/13에서 개발한 총 5건의 권고안이 QKDN에 대한 전반적인 내용을 다루고 있는 핵심 권고안이고, 앞으로는 QKDN 핵심 권고안을 바탕으로 세부적인 기술항목에 대한 표준안으로 영역을 확대시켜 나가는 형태가 될 것임
- Q16/13이 QKDN 전반적인 표준화를 주도하고 있고, 보안 부분 세부 기술은 SG17에서 주도하고, QoS 측면은 Q6/13, 그리고 조금 장기적인 측면에서 전반적인 기술에 대한 이해와 표준화 연구항목을 발굴해 나가는 것은 FG-QIT4N에서 진행 중인 상황에서, 향후 다음과 부분에 대한 표준화 필요
- 세부 기술에 대한 별도 권고안 개발
  - 요구사항 및 구조 관련 권고안 개발을 진행하면서 이슈가 되었던 내용에 대한 별도 권고안 개발. 예를 들면 Synchronization, 키 관리(KM)나 운용관리(CM) 관점에서도 QKD를 효율적으로 운용하기 위한 특정 기술항목을 발굴. CM 문서의 child 문서로 SDNC 문서를 개발하고 있듯이 기계학습(ML) 기술을 CM에 적용하거나, CM의 특정 기능에 대한 상세 메커니즘이나 좀 더 구체성이 있는 기술 아이템에 대한 표준개발이 가능할 것임
- 구조 문서에 대한 후속 권고안
  - KM, CM등에 있는 구조 측면 내용을 후속 권고안 형태로 해서 권고안 내용을 상세 프로토콜 수준으로 깊이(depth)를 좀 더 들어가는 형태가 됨
- 오픈 소스 연계 표준 개발을 위한 연구항목 제안

- 한국에서 시범사업이 진행되고, 오픈 소스 연계 표준에 대한 필요성이 증가됨에 따라 오픈 소스에 대한 분석 및 표준 측면에서 고려할 사항에 대한 기술보고서 개발, 이를 바탕으로 추후 필요 시 권고안 작업을 진행, 추후 시험 및 인증 등에 대한 이슈에 대응

- 사용자 네트워크 (User network) 측면에서 QKDN 지원
  - 지금까지는 QKDN 중심으로 문서를 개발했는데, 관점을 달리해서 기존 통신사업자가 5G와 같은 통신망에 QKDN을 어떻게 도입해서, 구체적으로 어떤 서비스가 가능할 지에 대한 솔루션 제시 필요. SG13에서 주도하는 5G 기술 측면에서 QKDN의 도입과 연동을 고려, 통신사업자가 필요로 하고 관심있어 하는 표준개발 진행
- QENS (Quantum Enhanced Networks and Services) 표준화
  - 차기 회기 Q16/13 ToR(Terms of Reference)에 양자 확장 네트워크 (Quantum Enhanced Network) 용어를 사용. 보안 관점의 QKD 기술 범주를 벗어나서 양자통신의 전반적인 측면에서 새로운 아이템 발굴이 필요

첨부1. 참고문헌

[1] TTA, "ICT 표준화 전략맵, 지능형 네트워크", ver.2020, 2019.

[2] 이지은, 상의정, 박춘걸, "양자암호 전달 네트워크 기능구조", TTA 저널, vol.190. 2020. 07/08.

[3] 윤빈영, "ITU-T SG15 양자키 분배 표준화 동향"ICT Standard Weekly, 제910호, 2019.