

양자암호통신 테스트베드 및 표준화 동향

| 작성 | SKT 김민형 매니저 (minhyung.kim@idquantique.com)



- o 『Al Network Lab 인사이트』는 인공자능, 클라우드, 5G, 양자정보통신 등 4차 산업 혁명의 핵심인 지능정보기술과 네트워크 신기술에 대한 동향을 간략하고 심도 있게 분석한 보고서입니다.
- o 본 연구보고서는 과학기술정보통신부의 방송통신발전기금조성사업, 한국정보화진 흥원의 미래네트워크선도시험망 구축·운영사업의 연구과제 결과이며, 한국정보화 진흥원/경기도경제과학진흥원과 공동 기획하였습니다.
- o 본 보고서의 내용의 무단 전재를 금하며, 가공인용할 때는 반드시 출처를 『한국 정보화진흥원(NIA)』이라고 밝혀 주시기 바랍니다.

발 행 처 한국정보화진흥원

발 행 인 문용식

기 획 한국정보화진흥원 지능형인프라본부 인프라기획팀

보고서 온라인 서비스 www.nia.or.kr



| (1) 5 | 보고서 요약5 |
|-------|----------------------|
| 보고 | 서 주요 내용 |
| (1) | 개요7 |
| (2) | 해외 양자암호통신 테스트베드 동향8 |
| (3) | 국내 양자암호통신 테스트베드 동향11 |
| (4) | 해외 양자암호통신 표준화 동향12 |

국내 양자암호통신 표준화 동향17

양자암호기술의 보안인증과 관련된 표준화 동향19

결론 …………………………19

보고서 요약

(5)

(6)

(7)

- 양자정보통신은 양자의 물리학적 특성을 정보통신에 적용하여 데이터의 초고 속처리, 초정밀, 고신뢰 전송이 가능하게 하여 4차산업혁명 시대에 국민에게 보다 빠르고, 안전하며, 정밀한 인프라를 제공하는 핵심 차세대 기술이다.
- 양자정보통신은 일반적으로 양자암호통신, 양자컴퓨터, 양자센서 등의 분야로 세분되며, 이중 양자암호통신은 중간정보 탈취, 불법 도감청 등을 원천 차단해 기존 통신 인프라의 보안성을 강화는 기술이다.
- 미국, 유럽, 중국, 일본 등 선진 주요국은 양자암호통신의 중요성을 일찍부터 인지하고, 양자정보통신과 관련된 중장기 정책 수립을 하고, 실험·시험망을 구성·운영하는 등 대규모 투자를 통해 기술개발 및 산업발전에 지원하고 있다.
- 본 보고서에서는 유럽과 일본에 구축·운영되어온 양자암호통신 관련 테스트베 드에 대해 알아보고, 최근 진행중인 표준화 동향에 대해 소개하고자 한다.

양자암호통신

암호통신 (보안통신)



양자암호키분배 (Quantum Key Distribution, QKD)

- 송신부에서는 전송 데이터를 암호 용 키를 이용하여 암호화하여 전송
- 수신부는 동일한 암호용 키를 이용 하여 암호화된 데이터를 복호화
- <mark>암호용</mark> 대칭 키의 분배 및 관리가 매우 중요
- 양자역학원리를 이용한 도청불가 기능으로 암호용 키를 안전하게 송 수신부에 분배
- 지속적인 암호용 키분배로 키를 주 기적으로 교체하여 안전성을 향상

보고서 요약

(1) 개요

• 양자암호 기술에 대해서 아직까지 많이 생소하다. 아직까지 인터넷만큼 우리에게 가까 이 다가온 기술은 아니지만, 앞으로 5G 네트워크의 확산과 함께 우리의 데이터를 안전 하게 지켜줄 차세대 기술 중에 하나이다.

(2) 해외 양자암호통신 테스트베드 동향

- 미국, 유럽, 중국, 일본 등 선진 주요국은 양자암호통신의 중요성을 일찍부터 인지하고, 80연대부터 본격적인 연구가 시작되어, 90년대 연구용 시제품이 개발되었고, 2000년 이후 부터는 양자정보통신과 관련된 중장기 정책 수립을 하고, 실험·시험망을 구성·운 영하는 등 대규모 투자를 통해 기술개발 및 산업발전에 지원하고 있다.
- 유럽에서는 2004년부터 2009년까지 단일광자 검출의 최적화, 표준화 및 테스트베드 구축을 목적으로 SECOQC라는 프로젝트를 진행하였다.
- 일본에서는 도쿄 QKD 네트워크는 국가의 시험망(JGN)을 활용하여 기존 SECOQC보다 개선된 양자키생성 및 안정성을 검증하였으며, 결과를 일반인들도 홈페이지에서 실시간으로 확인 할 수 있도록 하고 있다.

(3) 국내 양자암호통신 테스트베드 동향

- 국내 테스트베드는 2016년 SKT가 양자암호통신 기술개발 기반 조성 및 신뢰성 검증 등을 위한 분당~용인구간 시험망을 구축하였다.
- 한국정보화진흥원은 2018년 국가시험망인 KOREN을 활용하여 SKT의 QKD와 국내 전송장비와 연동하여 서울~판교간 양자암호통신 기술을 적용하였다.

(4) 해외 양자암호통신 표준화 동향

• 유럽전기통신표준화협회(ETSI)에서 양자키 분배기술의 표준은 ISG중 하나인 QKD가 양자키 분배기술과 관련하여 9개의 그룹규격을 제정했고, 2개의 그룹규격이 신규로 논

의되고 있다.

• ITU-T의 SG13과 SG17에서 양자키 분배 시스템으로 실제 네트워크를 구성하고 사용하는 부분에 있어서 필요한 부분을 중심으로 표준화를 진행해 나가고 있다.

(5) 국내 양자암호통신 표준화 동향

• 국내에서도 TTA에 ETSI 표준을 그대로 인용하여 국내 영문표준으로 만들었고, 양자키 분배와 관련한 표준 2건도 제정이 되었다.

(6) 양자암호기술의 보안인증과 관련된 표준화 동향

- 양자암호통신 관련 시스템의 상호운용성 확보도 중요하지만, 해당 기술을 구현한 장비가 정말로 신뢰하고 사용할 수 있는지에 대한 부분을 검증하는 것도 중요하다.
- 현재 IT 시스템에서 제품의 보안 인증과 관련된 규격은 공통평가기준과 암호모듈 검증 제도 두 가지로 구분되어 표준화를 진행하고 있다.

(7) 결론

- 해외에서는 일찍부터 양자암호통신 관련 연구, 제품개발, 테스트베드를 통한 시험검증을 진행 해왔고, 국내의 경우 다소 늦었지만, 글로벌 경쟁력을 지닌 광전송, 5G 및 반도체 제조기술 강국으로서 우리의 장점과 시너지 창출시 세계 시장 선도가 가능 할 것으로 예상된다.
- 표준화는 양자키 분배 시스템을 중심으로 선택과 집중을 통해, 통신사와 연구소간 협력 이 이루어 범국가적 전략적 표준화 작업이 이루어진다면, 우리나라가 표준 선도 뿐아니라 제품 상용화에 한걸음 더 빨리 다가갈 수 있을 것이다.

※ 시사점

- · 국내의 경우 양자암호통신에 관한 연구가 다소 늦었지만, 글로벌 경쟁력을 지닌 광전송, 5G 및 반도체 제조기술 강국으로서 우리의 장점과 시너지 창출시 세계 시장 선도가 가능 할 것으로 예상
- · 표준화의 영역은 기관별 요구사항이 다를수 있지만 핵심 기술을 중심으로 **선택과** 집중을 통해, 통신사와 연구소간 협력이 이루어 범국가적 전략적 표준화 작업이 이루어 진다면, 우리나라가 표준 선도와 제품 상용화를 통한 세계시장 주도 가능

양자암호통신 테스트베드 및 표준화 동향

주 요 내 용

(1) 개요

- 양자암호 기술에 대해서 아직까지 많이 생소하다. 아직까지 인터넷만큼 우리에게 가까 이 다가온 기술은 아니지만, 앞으로 5G 네트워크의 확산과 함께 우리의 데이터를 안전 하게 지켜줄 차세대 기술 중에 하나이다.
- 가트너는 양자컴퓨팅 기술이 5~10년이내에 시장이 올것이라 예측 했다. 양자암호통신은 양자컴퓨팅보다는 기술 성숙도가 높고 이미 상용화 제품이 출시되어 있어, 빠르면 2년 후 본격적으로 세계시장이 형성되고, '25년에는 약 14조원(12.5억달러)에 이를 것으로 전망된다.
- 양자암호 기술은 양자컴퓨터가 기존의 비대칭 키 암호체계를 무력화 시킬 수 있다는 사실에서 출발하고 있다. 양자컴퓨터는 암호학에서도 중요한 역할을 하지만, 인공지능, 머신러닝, 퀀텀시뮬레이션 등의 분야에서도 중요한 역할을 할 것으로 예상되고 있다. 구글, IBM, Microsoft 등이 이미 양자컴퓨터를 개발하고 있으며, 일부 회사는 클라우드 형태로 시험환경과 서비스를 제공하고 있다. 하지만, 아직까지 기존의 비대칭 암호체계를 무력화 할 수 있는 양자컴퓨터가 나온 것은 아니다. 하지만 보호하려는 정보의생명주기가 길다면 지금부터 준비하지 않으면 정말 양자컴퓨터가 나왔을 때 그 정보를보호할 수 없게 된다.
- 이러한 양자컴퓨터 출현의 가능성으로 세계적으로 그 위협을 제거하거나 약화시키는 방향으로 기술개발이 이루어지고 있다. 우선 키 교환 시 주로 사용하는 비대칭 키 알고 리즘을 전혀 사용하지 않고 두 지점 간에 정보공학적으로 안전한 키 교환을 제공하는 기술인 양자키 분배 기술이 있고, 양자컴퓨터로도 그 암호를 해독하는데 오랜 시간이 걸린다는 양자내성암호 알고리즘이 있다.
- 양자키 분배 기술은 양자역학의 원리를 이용하여 서로 약속한 송신자와 수신자가 아니라면 중간에서 정보를 빼내갈 수 없는 기술이다. 양자키 분배 기술은 미국과 유럽의 여러 나라들에서 2000년대 후반부터 시험망이 만들어지고 연구가 수행되었다. 그리고 그구현방법도 BB84, Decoy, CV-QKD, MDI-QKD 등 다양한 기술이 나와 있는 상황이다. 또한 2010년대 중반부터 중국은 베이징에서 상해까지 이르는 세계에서 가장 긴 암

자암호통신망을 구축하였다. 이러한 시험망의 확산과 상용화 연구 등으로 장치간의 연동과 표준화에 대한 요구가 점차 증가하고 있고, 국내의 TTA를 비롯한 ETSI, ITU, ISO등에서 양자키 분배 기술에 대한 표준화가 이루어지고 있다.

• 양자내성암호는 Post Quantum Cryptography(PQC) 또는 Quantum Safe Cryptography(QSC)라는 명칭으로 표준화가 이루어지고 있으며, 양자컴퓨터가 나오 더라도 기존의 비대칭 키 암호화 알고리즘과는 달리 오랜 연산시간이 소요되어 안전한 알고리즘을 말한다. PQC 알고리즘은 많은 종류가 연구되고 발표되었으나 아직까지 표준으로 통용되는 알고리즘은 없다. 현재 NIST에서 Cryptography Competition을 통해 PQC 알고리즘을 제안 받고 표준화를 추진하고 있다.

(2) 해외 양자암호통신 테스트베드 동향

- 미국, 유럽, 중국, 일본 등 선진 주요국은 양자암호통신의 중요성을 일찍부터 인지하고, 80연대부터 본격적인 연구가 시작되어, 90년대 연구용 시제품이 개발되었고, 2000년 이후 부터는 양자정보통신과 관련된 중장기 정책 수립을 하고, 실험·시험망을 구성·운 영하는 등 대규모 투자를 통해 기술개발 및 산업발전에 지원하고 있다.
- 테스트베드는 기술개발의 순서에 따라 실험망(기술개발 및 시연) → 시험망(장거리 시연 및 네트워크 안정성 시험) → 시범망(응용 서비스 실증) → 상용망(상용서비스 제공)
 으로 구분할 수 있다. 다음은 각국의 양자암호통신 테스트베드 구축현황을 정리하였다.
- 미국의 DARPA Project를 시작으로 2002년부터 실험망이 구성되었고, 2004년 유럽에서 많은 연구팀이 모여 QKD 네트워크를 구성하였으며, 일본에서는 2010년 유럽 테스트베드를 벤치마크하여 도쿄 양자암호실증망을 구축하였다.
- 중국도 2010년부터 중국과기대에서 테스트베드를 구축하고, 최근 베이징 ~ 상하이간 양자 백본 구축을 완료하여 상용서비스를 제공하고 있다. 이러한 네트워크 구축 운영 경험은 중국이 표준화를 위하여 ITU-T에 제시한 아키텍쳐, 인터페이스 등에 많은 영향을 주었다.
- 본 보고서는 유럽에서 진행된 SECOQC와 도쿄 QKD 네트워크 테스트베드에 대해 살펴보고자 한다.

[해외 양자암호통신 테스트베드 구축 동향]



| 국가 | 실험망 | 시험망 | 시범서비스 실증망 | 상용서비스망 | | |
|----|--|---|--|----------------------------------|--|--|
| 미국 | • DARPA 시연 ('02- '07) | ** ~ おけけ ^ – 위 () け) (' | | • 퀀텀익스체인 지월가 서비 스 (18-) | | |
| 유럽 | • SECOQC 시연 ('04-'08) • 스위스선거시연 ('07) | 스위스퀀텀 안정성 시험 ('09-'11) 이탈리아 장거리 시험망 ('13-'16) | • AVDA 2,800km전송서비스 (18) | _ | | |
| | (01) | Quantum Internet Allian | | | | |
| 일본 | • Tokyo QKD Network 실험/시험망 | ('10-) 개방형 | • NEC데이터센터 서비스('15) • 도시바-동북대 의료데이터 서 비스('15) • H-LINCOS ('18) | - | | |
| 영국 | • 아다시트랄-입스위치 시연 ('14) | • 브리스톨-캠브리지 장거 리 시험('13-'18) | • 아다스트랄-캠브리지 은행서 비스 (17) | _ | | |
| 중국 | • 중국과기대 시연('09) | • 중국과기대 5개 노드 네트 워크(10) • 허페이(12), 진안(13) 네 트워크 시험 | • 상해-북경 간 QBN('12-'17)으로 의 양자암호통신 서비스('18-) | 로 은행망, 통신 사 | | |

(7) SECOQC (SEcure COmmunication based on Quantum Cryptography)

- 유럽에서는 2004년 단일광자 검출의 최적화, 표준화 및 테스트베드 구축을 목적으로 SECOQC라는 프로젝트에 착수하였다.
- 2008년 많은 연구팀이 오스트리아 빈 지역에 모여 QKD 네트워크를 형성하기 위해 중간에 6개의 노드들을 구성하고, 각 노드간 QKD 프로토콜은 다양하게 구성하여 약 285Km 구간의 Quantum Back bone Network(QBB)를 총 1,100만유로(144억원)

를 투입하여 구축 하였다.

- 각 노드간에는 COW방식(Coherent one way), 위상을 이용한 BB84방식, Plug&Play 방식, 얽힘방식(Entanglement based QKD), CV방식(Continuous Variable), 그리 고 자유공간을 이용한 방식(Free Space)의 프로토콜을 각각 사용하였다.
- 2009년 25km구간에서 최대 1kbit/s 의 양자암호키 생성 및 연동 실험을 추진하였고, 신뢰노드 적용 가능성 및 문제점 등을 점검하였으며, 테스트베드 운영 경험을 기반으 로 현재 ETSI ISG QKD 표준이 제정 되었다.
- 결국 SECOOC는 각 링크별로 다양한 OKD기술을 시험하고 비교하였으며 네트워크 구 성에 필요한 항목을 도출했다는데 의미를 가지며, 향후 ETSI가 양자암호통신의 표준화 를 선도하는 계기가 되었다.

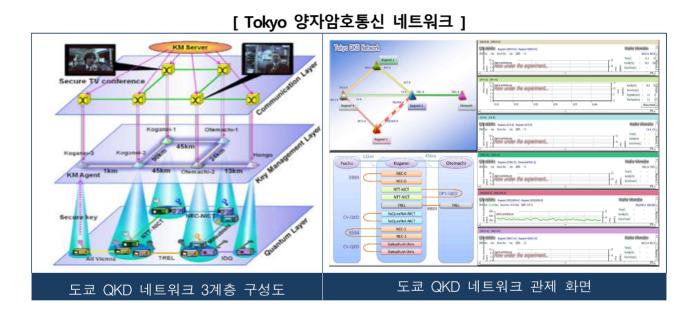
[SECOQC Project의 양자암호통신 네트워크]



(나) 도쿄 QKD 네트워크

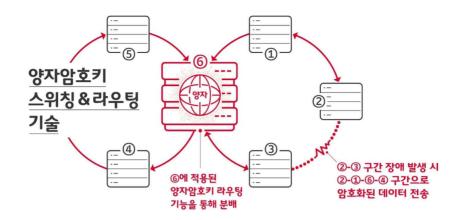
- 일본은 국립정보통신연구원(National Institute of Information and Communications Technology - NICT) 주관으로 도쿄 시내 양자암호통신 네트워크를 구축('10년), 45Km 광케이블 구간에서 294kbs의 전송속도로 양자키분배 성공하고, 동영상 암호전 송에 성공('12년)하였다.
- NICT, NEC, 미쯔비시 및 NTT 등이 참여하여 도쿄 중심부에 6개의 링크(총연장 218km) 양자암호통신 네트워크를 일본의 국가시험망인 JGN(Japan giga Bit Network 2 Plus)의 광케이블을 활용하여 구축하였다.

- 양자암호 네트워크의 구성은 EU의 기술개발 프로젝트(SECOQC)와 유사한 3-layer 아 키텍처를 사용하여 점대점(1:1) 통신 백본망 형태로 구성하였으며, UOCC(Updating Quantum Cryptography and Communications - NICT가 주도하는 양자암호 및 양자통신에 관련된 국제학회)에서는 일회용 암호화(one-time pad encryption)에 대 한 실제시연에 성공('10년)하였다. 이후 실제 사용자에게 확대되어 홈페이지 (www.tokyogkd.ip)를 통해 암호키 생성속도에 대한 확인('15년)이 가능하도록 구성하 고 있다.
- 도쿄 OKD 네트워크는 국가의 시험망을 활용하여 기존 SECOOC보다 개선된 양자키 생성 및 안정성을 검증하였고, 키 관리 계층을 적용하였으며, 양자 키를 이용하여 의료 정보를 안전하게 분산저장하여, 중요 데이터의 가용성을 높이는 실증을 했다는데 큰 의 의가 있다.



(3) 국내 양자암호통신 테스트베드 동향

- 국내 테스트베드는 2016년 SKT가 양자암호통신 기술개발 기반 조성 및 신뢰성 검증 등 을 위한 분당~용인구간 시험망을 구축하였고, 최근 국책과제를 통해 두개의 링 네트워크 간에 키를 라우팅하고 스위치할 수 있는 기술을 적용하였다.
- 2016년, 세종~대전간 LTE 상용망에 양자암호 기술을 적용하여 세종시 일원에 음성, 데이터 통신에 대해서 보안기능을 제공하였으며, 2019년에는 5G 개통과 함께 성수~ 둔산간 5G 상용망에 양자암호기술을 적용하였다.



- 공공분야에서는 한국과학기술정보연구원이 운영하는 SuperSIRen과 KREONET에 양 자암호기술의 적용하여 위성데이터의 일부 전송구간과 유전체 데이터의 DR센터 연결 의 전송 구간에 적용되었다.
- 한국정보화진흥원은 2018년 국가시험망인 KOREN을 활용하여 SKT의 OKD와 국내 전송장비와 연동하여 서울~판교간 양자암호통신 기술을 적용하였다. 국내 전송장비는 코위버의 ROADM과 우리넷의 POTN 장비에 각각 10Gbps급 암호화 모듈로 암호화 통신을 적용하고 있다.

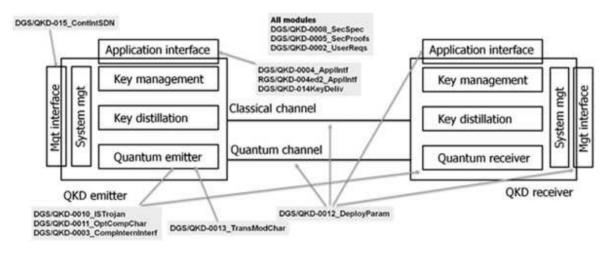
(4) 해외 양자암호통신 표준화 동향

- 양자암호기술은 크게 양자키 분배기술(Quantum Key Distribution QKD)과 양자 내성 암호 기술(PQC) 두 가지로 나누어진다. 양자키 분배기술은 양자키 분배를 위한 표준과 양자키 이용하여 네트워크를 구성하고 사용하는데 필요한 기술로 표준화가 진 행되고 있으며, 양자 내성 암호 기술은 표준 알고리즘을 선정하기 위한 방향으로 표준 화가 진행되고 있다.
- 해외에서는 ETSI, ITU-T, ISO/IEC 등의 표준화 기관이 국제 표준화 작업을 활발하게 진행하고 있으며, IEEE는 미국의 양자정보통신 기술 비공개 전환으로 사실표준에서의 표준화 추진이 불확실하다.
- (가) 유럽전기통신표준화협회(European Telecommunications Standards Institute ETSI)
 - 양자키 분배기술의 표준은 ETSI의 ISG(Industry Specification Group)중 하나인 QKD가 양자키 분배기술과 관련하여 9개의 그룹규격을 제정했고, 2개의 그룹규격이

신규로 논의되고 있다.

- 아래 그림에서와 같이 ETSI 규격은 QKD 시스템을 중심으로 인증과 유지보수 위주로 규격이 제정되었다. GS QKD 002; Use Cases를 기반으로 각 Use Case에서 필요한 기술들에 대해서 규격을 제정하고 있다. 주로 QKD 시스템 자체에 대한 규격을 정하고 있으며, GS QKD 004의 경우 API 수준에서 양자키를 외부에서 가지고 가는 규격을 정의하였는데, 구현의 구체성이 부족하여 잘 사용하지 않고 있다가, 2019년 2월에 GS QKD 014 Protocol and data format of REST-based key delivery API가 발표되면서 유럽과 미국의 제조사를 중심으로 해당 규격을 지원하고 있으며 QKD 시스템과 Security Application을 연동할 때 손쉽게 사용할 수 있을 것으로 예상된다.
- 최근에는 SDN 환경에서 양자 네트워크를 관리하기 위한 GS QKD 015 Control Interface for SDN 이 제안 표준화를 진행하고 있다. 이 표준으로 동적으로 양자 네트워크의 설정을 변경하여 사용하자 원하는 종간간 양자키를 생성하고 필요시 양자키가 중계되는 경로까지도 동적으로 설정하고자 하는 것이다. 아래 그림은 ETSI의 표준화현황을 표시한 것이다.

[ETSI 표준화 현황]



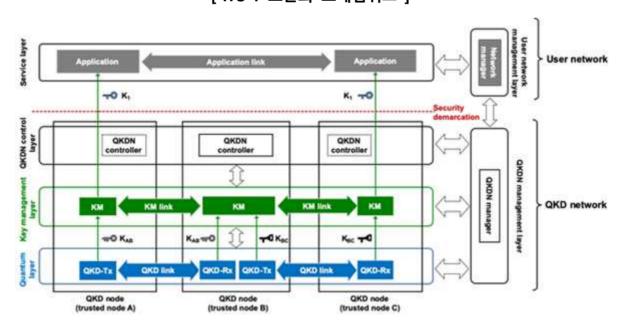
| 번호 | 표준명 | 버전 | 발행일 |
|-----|--|-------|--------|
| 012 | ■ Device and Communication Channel Parameters for QKD Deployment | 1.1.1 | ′19.2 |
| 014 | ■ Protocol and data format of REST-based key delivery API | 1.1.1 | ′19.2 |
| 007 | ■ Vocabulary | 1.1.1 | '18.12 |
| 003 | ■ Components and Internal Interfaces | 2.1.1 | ′18.3 |
| 011 | ■ Component characterization | 1.1.1 | '16.5 |
| | : characterizing optical components for QKD systems | | |
| 005 | Security Proofs | 1.1.1 | ′10.12 |
| 800 | QKD Module Security Specification | 1.1.1 | '10.12 |
| 004 | ■ Application Interface An update is in preparation | 1.1.1 | '10.12 |
| 002 | ■ Use Cases | 1.1.1 | '10.6 |

- ETSI의 그룹규격이 현재까지는 가장 많은 표준 규격을 가지고 있으며 필요한 연구가 가장 먼저 진행되었다.
- ETSI에는 양자암호기술과 관련된 또 하나의 Working Group(WG)이 있는데 Cyber Security 위원회에 속해 있는 QSC WG가 그것이다. QSC WG는 ISG QKD보다 이른 2015년에 ISG QSC로 결성되어 시작을 했지만, 2017년에 ISG에서 TC로 편입되었다. 하지만, 아직까지 추가적인 표준 아이템은 없고, 미국의 NIST(National Institute of Standards and Technology 국립표준기술연구소), 캐나다의 IQC(Institute for Quantum Computing 양자컴퓨팅연구소)와 함께 Post Quantum 시대를 대비한 기술에 대한 논의를 진행하고 있다.
- ISG에서 제정하는 그룹규격(Group Specification GS)은 기술위원회(Technical Committee TC)에서 제정하는 기술규격(Technical Specification TS)과 달리 강제사항이 아니기 때문에 그 적용에 있어서는 영향력이 떨어진다고 볼 수 있다. 이러한 한계를 극복하고자 보안제품으로 인증을 받기 위한 다른 규격들이 ISO를 통해서 제안되고 있다.

(나) ITU-T

- 양자키 분배기술은 양자신호를 이용하여 키를 분배하는 기술이기 때문에 일반 광통신에 비해서 전송거리가 상대적으로 짧고 일반 광통신과 달리 신호를 증폭하여 보낼 수 없기 때문에 장거리 전송이 불가하다. 이러한 한계를 극복하기 위해서 두 양자키 분배 구간을 연동하여 키를 전송하는 TR(Trusted Repeater)기술을 이용하여 장거리 전송을 가능하게 한다. 하지만, 이 기술은 모두 양자기술을 이용하는 것이 아니라 연동하려는 구간에서 각각 생성된 양자키를 이용하여 TR에서 키를 연동하는 기술을 사용한다. 이렇게 양자키 분배 시스템 이외에 키를 연동하는 계층이 별도로 존재하기 때문에 새로운 계층에 대한 표준화가 필요하게 된다.
- 이 계층에 대해서 아직까지 용어가 통일되지 않지만, Key Management Layer, Control Layer 등으로 불린다. 이러한 새로운 계층에서의 인터페이스와 실제로 양자 키를 사용하기 위한 장비들 간의 연결 관계 및 프레임웍을 정의한 규격이 ITU-T를 중심으로 제안과 논의가 되고 있다. 이 분야에서는 국내 통신사의 참여가 활발하다.

- ITU-T의 SG13과 SG17에서 각각 KT와 SKT가 주도적인 표준화 활동을 벌이고 있으 며 앞에서 설명한 바와 같이 양자키 분배 시스템에 대한 규격화는 다른 표준화 단체의 것을 사용하고 실제 네트워크를 구성하고 사용하는 부분에 있어서 필요한 부분을 중심 으로 표준화를 진행해 나가고 있다.
- ITU-T SG13은 미래 네트워크에 대한 표준을 정하는 연구그룹으로 Q16에서 양자네트 워크 프레임웍에 대한 표준화를 추진하고 있으며, KT에서 제안한 안이 현재 Y.3800 Framework for Networks supporting QKD 라는 명칭으로 2019년 7월 중순부터 동의절차에 들어가 다른 나라들의 특별한 반대가 없다면 2019년 9월경 양자네트워크 관련 표준이 될 전망이다.
- Y.3800에서는 양자 네트워크 구성을 위한 기본 프레임웍을 아래 그림과 같이 제시하 고 있다. 아래 그림의 내용은 표준으로 완전히 제정 될 때까지 변경될 수 있다. Quantum layer에서 각 노드 간에 생성된 키를 Key management layer에서 저장, 전달, 중계 등을 수행하며, QKDN(QKD Network) control layer에서 Key management에 필요한 제어를 담당한다.

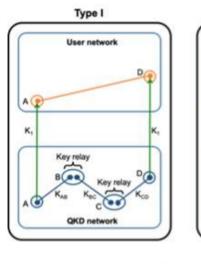


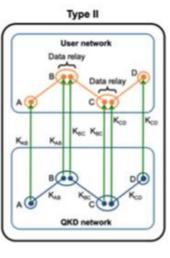
[ITU-T 표준화 프레임워크]

• 이러한 프레임웍을 기반으로 QKD 네트워크 계층과 사용자 네트워크간의 사용 예를 세 가지로 제시하고 있는데, 어느 네트워크에서 종단간 키 중계를 했는지에 따라서 구 분된다.

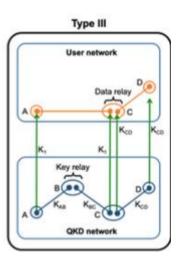
- 첫 번째는 QKD 네트워크에서 키를 중계하여 사용자 네트워크에서는 종단간에서만 키를 공급 받는다.
- 두 번째는 사용자 네트워크에서 매 구간 QKD 네트워크에서 공급받아 종단간 전송할 때 중간 노드에서 반복적으로 암호화를 수행한다.
- 마지막 방법은 앞으로 두 가지를 혼합해서 사용하는 것이다.

[종단간 키 중계 방식]





QKD device QKD link QKD node



• 중국은 위에서 제시한 프레임웍을 기반으로 QKDN의 Architecture와 QKDN을 위한 Software Defined Network Control 표준화를 진행하고 있다. 일본은 Key

management layer를 중심으로 Key 전달 등의 표준화를 진행하고 있다.

- ETRI와 KT는 QKD network control layer와 QKD network management layer 를 상세히 표준화를 진행하고 있다. SG13은 QKD 자체 기술이 아니라 QKD를 이용한 네트워크 구조에 대해서 표준화를 진행하고 있다. QKD network를 구성하는데 필요한 표준의 제정이 2020년 말이면 어느 정도 모양을 갖출 것으로 예상되고 있다.
- SG17에서는 양자암호 네트워크에서 필요한 보안관점의 표준들을 논의하고 있다. 주로 KMS(Key Management System)와 관련된 보안 사항에 대해서 표준화가 논의 되고 있다. 왜냐하면 QKD 자체의 표준에는 이미 ETSI와 ISO에서 상당 부분 논의 되고 있어 ITU-T에서는 해당 규격에 대한 내용을 준용하거나 수용하는 방향으로 표준화가 진행되고 있고, 다른 표준화 단체에서는 KMS분야에 대해서 표준화를 진행하고 있지 않

기 때문이다.

• SKT는 "Quantum Noise RNG(Random Number Generator) Architecture"과 "Security framework for QKD in telecom network" 두 가지 아이템에 대해서 표 준화를 진행하고 있다. "Quantum Noise RNG Architecture"는 QRNG의 일반적인 구조와 구성요소에 대해서 정의하고 있으며, 양자암호 기술의 보안성의 출발점이 되고 있다. 그리고 "Security framework for QKD in telecom network"은 QKD를 통신 사업자망에 구성할 때 고려할 보안요소에 대해서 기술하고 있다. 이는 KMS와 KMS간 의 연결, KMS와 관리 인터페이스의 연결, KMS와 OKD간 연결, KMS와 외부 어플리 케이션간의 연결에서 고려할 사항에 대한 내용을 표준화하고 있다. 추가적으로 중국, 일본과 함께 QKD 네트워크에서 보안 요구사항에 대해서도 표준화가 진행되고 있다.

(5) 국내 양자암호통신 표준화 동향

- 국내에서도 한국정보통신협회(TTA)에서 표준을 제정하고 있다. 주로 ETSI 표준을 그 대로 인용하여 국내 영문표준으로 만들었고, 양자키 분배와 관련한 표준 2건도 제정이 되었다.
 - TTAK.KO-12.0329-Part1 양자 키 분배 제1부 : 일반
 - TTAK.KO-12.0329-Part2 양자 키 분배 제2부 : BB84 프로토콜
 - TTAE.ET-GS QKD 003 양자 키 분배: 구성 요소 및 내부 인터페이스
 - TTAE.ET-GS QKD 004 양자 키 분배망: 응용 인터페이스
 - TTAE.ET-GS QKD 008 양자 키 분배: 모듈 보안 규격
 - TTAE.ET-GS QKD 011 양자 키 분배: 구성 요소 특성화 : QKD 시스템의 광학 구성 요소 특성화
- TTAK.KO-12.0329 규격은 QKD 표준은 제1부 일반, 제2부 BB84 프로토콜로 구성 된다. 제1부 일반에서는 QKD의 개념을 바탕으로 일반적 모델을 정립하고, 다양한 OKD 프로토콜을 포괄할 수 있는 단계별 절차와 안전성 요구사항을 제시한다. 제2부인 이 표준은 QKD의 구현 안전성을 높이는 디코이 기법이 적용된 BB84 프로토콜의 단 계별 세부 절차와 안전성 고려사항을 제시한다.
- TTAE.ET-GS QKD 003, 004, 008, 011은 ETSI GS QKD 003, 004, 008, 011을 그대로 표준으로 인용하여 정의한 것으로 양자암호 시스템의 구성요소 및 평가에 관한

사항에 대해서 국내 표준으로 인정하고 있다. 이 외에도 ETSI GS QKD에 추가로 재정 된 013, 014 등도 TTA 표준으로 등록 될 것을 기대된다.

• 이 외에 양자키 분배 시스템에 대한 보안 요구사항에 대한 표준이 진행되고 있다. 이 표준을 통해서 양자키 분배 시스템을 기존의 암호모듈 검증 제도로 수용할 수 있는 계 기가 되기를 희망한다.

(6) 양자암호기술의 보안인증과 관련된 표준화 동향

- 양자암호기술도 보안과 관련된 기술이기 때문에 표준 준수를 통한 장비간의 상호 운용 성 확보도 중요하지만, 해당 기술을 구현한 장비가 정말로 신뢰하고 사용할 수 있는지 에 대한 부분을 검증하는 것도 중요하다.
- 현재 IT 시스템에서 제품의 보안 인증과 관련된 규격은 공통평가기준(CC, Common Criteria)과 암호모듈 검증제도(CMVP, Cryptographic Module Validation Program) 두 가지로 구분될 수 있다.
- 공통평가기준은 IT 제품의 보안기능성과 평가 과정에서 그 제품들에 적용되는 보증수 단에 대한 공통의 요구사항을 제시함으로써 독립적으로 수행된 보안성 평가의 결과물 을 비교할 수 있도록 하는 것이다. 중국은 ISO/IEC JTC1/SC27에 QKD 표준화 프로 젝트를 제안하였다. 이는 공통평가기준 평가체계를 이용하여 QKD 시스템의 보안성을 평가하고자 한다.
- 현재까지는 다양한 QKD 기술에 대한 소개와 함께 QKD의 보호자산별 주요 위협을 정리하고 있다. 공통평가기준은 공통의 요구사항을 제시하는 방식으로 접근하다 보니 너무 일반화된 사항들만을 다루게 되어 실질적인 구현의 적합성을 다루지 못하는 문제 가 있기도 하다. 이러한 문제를 해결하기 위해서 공통평가기준을 통해서 IT제품을 평 가할 때도 암호기능은 별도의 암호모듈 검증제도를 통과한 제품을 같이 쓰도록 요구하 고 있다.
- 또 다른 한편으로는 양자키 분배시스템을 암호모듈로 보안 시스템 구성의 안전성과 구 현 적합성을 평가하는 방향도 있다. 앞에서 소개한 TTA의 표준화 동향 중에 양자키 분배 시스템 보안 요구사항이 양자키 분배 시스템을 암호모듈 검증제도에 좀 더 가까 지 다가 갈수 있게 해주는 표준이라고 불 수 있다. 양자키 분배시스템을 암호모듈로 본다면 양자키 분배 시스템에 대한 보안 요구사항과 그 요구사항에 따라서 구현이 적

합하게 되는지 검증 할 수 있게 된다.

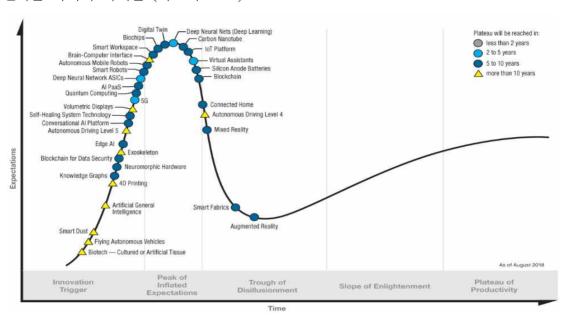
(7) 결론

- 양자암호통신 테스트베드와 기술 표준화 동향을 각각 살펴보았다. 해외에서는 일찍부 터 양자암호통신 관련 연구, 제품개발, 테스트베드를 통한 시험검증을 진행 해왔음을 확인할 수 있다. 국내의 경우 다소 늦었지만, 글로벌 경쟁력을 지닌 광전송, 5G 및 반 도체 제조기술 강국으로서 우리의 장점과 시너지 창출시 세계 시장 선도가 가능 할 것 으로 예상된다.
- 표준화의 영역은 표준화기관별로 조금씩 다르지만, 양자키 분배 시스템에 필요한 요소 들에 대해서 표준화가 이루어지고 있음을 확인할 수 있다. 양자키 분배 시스템은 두지 점간에만 사용하는 것이 아니라 네트워크 형태로 서비스 되는 모델을 가지고 표준화가 진행되고 있다. 이러한 구조와 보안 요구사항에 대한 표준화를 중심으로 선택과 집중을 통해, 통신사와 연구소간 협력이 이루어 범국가적 전략적 표준화 작업이 이루어진다면, 우리나라가 표준 선도 뿐아니라 제품 상용화에 한걸음 더 빨리 다가갈 수 있을 것이다.
- 양지키 분배 시스템이 확산되기 위해서는 이 시스템이 기존에 존재하는 보안인증 제도 에 수용되어서 소비자 입장에서는 인증을 받은 제품에 대해서 안전승과 구현의 적합성 을 보증 받고, 연동 인터페이스의 표준화를 통해 장비간의 상호호환성을 확보하여 중복 투자를 막을 수 있을 것으로 기대한다. 아직 양자암호 기술에 대한 표준화는 계속 진행 중이므로 관심을 가지고 지켜봐야 할 것이다.

양자암호통신 테스트베드 및 표준화 동향

주요 통계 사항

[1] 최신기술 하이퍼 사이클 (가트너 2018)



[1] 양자정보통신기술 분야별 세계 시장 전망(ICT 기술로드맵 2023)

(단위: 백만달러, 십억원, 1\$=1,100원)

| 구분 | | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | CAGR (19-25) |
|-------|--------|------|------|-------|-------|-------|--------|--------|--------|--------|-----------------|
| 양자통신 | 세계 | 48 | 83 | 158 | 323 | 1,957 | 2,482 | 3,385 | 6,759 | 12,266 | 106.5% |
| | 국내*** | 1 | 5 | 10 | 20 | 38 | 48 | 66 | 132 | 239 | 69.7% |
| 양자센서/ | 세계**** | 추정불가 | 추정불가 | 271 | 370 | 506 | 691 | 943 | 1,283 | 1,746 | 36.4% |
| 이미징 | 국내** | 0 | 0 | 4 | 5 | 7 | 10 | 14 | 20 | 28 | 41.1% |
| 아지커프티 | 세계**** | 추정불가 | 추정불가 | 3,602 | 4,526 | 5,940 | 7,672 | 10,462 | 13,831 | 17,882 | 30.6% |
| 양자컴퓨팅 | 국내** | 0 | 0 | 48 | 62 | 84 | 112 | 159 | 217 | 290 | 35.0% |
| 문니 | 세계 | 추정불가 | 추정불가 | 4,031 | 5,219 | 8,403 | 10,845 | 14,790 | 21,873 | 31,894 | 41.2% |
| 합계 | 국내 | 1 | 5 | 62 | 87 | 129 | 170 | 239 | 369 | 557 | 44.4% |

^{*} 출처: Quantum Encryption Systems Markets 2017-2026(CIR Market Report, 2017,6), Quantum Sensor Market 2017-2025(Acute Market Reports, 2017), Quantum Computing Technologies & Global Market 2017-2024(Homeland Security Research Corp., 2017), Global Quantum Computing Market, Industry Analysis and Opportunity Assessment 2017-2025(Persistence Market Research, 2017)

^{**} 양자정보통신 국내시장은 양자암호통신 아시아 시장에서 한국이 차지하는 비율(5.384%, 세계시장기준 1.95%)을 일괄 적용(The 2016-2021 World Outlook for Quantum Cryptography, 2015)

^{***} 양자통신 국내시장은 시장보고서 전망치[Quantum Encryption Systems Markets 2017-2026(CIR Market Report, 2017.6)]에 18년 자체 추정치를 적용하여 보정

^{****} 양자컴퓨팅 세계시장은 두 보고서의 평균으로 산출하였으며 HSRC 보고서는 정부지원금(Government Funded RDT&E) 포함(17-18년은 보고서 발간 시점 상 추정치이므로 제외)

양자암호통신 테스트베드 및 표준화 동향

참 고 문 헌

- [1] 곽승환, 양자키 분배기술 동향과 SK텔레콤 개발 현황, 2015년 6월
- [2] 박성수, 송호영, 양자정보통신기술 현황과 전망, ETRI, 2019년
- [3] 임용재 외 5명, 양자암호통신 기술 소개 및 동향, IITP ISSUE REPORT
- [4] https://www.etsi.org/technologies/quantum-key-distribution
- [5] ETSI GS QKD 002 UserReqs
- [6] ETSI GS QKD 003 CompInternInterf
- [7] ETSI GS QKD 004 ApplIntf
- [8] ETSI GS QKD 008 SecSpec
- [9] ETSI GS QKD 014 KeyDeliv[2] SG17-TD1950 Update of TR.sec-qkd based on the gap analysis between ETSI/ISO standardization activities and the proposed work at ITU-T SG17 on QKD 2019 01
- [10] SG17-TD1979 Proposed texts for draft X.qrng-a: Quantum Noise Random Number Generator Architecture 2019 01
- [11] Y.3800(SG13-TD-WP3-0264 Draft new Recommendation ITU-T Y.3800 "Framework for Networks supporting Quantum Key Distribution"
- [12] TTAK.KO-12.0329 Part1 양자 키 분배 제1부: 일반
- [13] TTAK.KO-12.0329 Part2 양자 키 분배 제2부: BB84 프로토콜
- [14] http://www.secoqc.net/
- [15] www.tokyoqkd.jp
- [16] https://www.etsi.org/technologies/quantum-key-distribution
- [17] https://www.itu.int/md/T17-SG13-181102-TD-WP3/en
- [18] https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx
- [19] Sasaki, M., et al. "Field test of quantum key distribution in the Tokyo QKD Network." Optics Express 19.11 (2011): 10387-10409

- [20] https://www.tta.or.kr/
- [21] https://www.iitp.kr/
- [22] https://www.gartner.com/