# 국내 통신사별 양자암호통신망 구축 및 대응전략 분석

유기성, 이원혁, 김용환
한국과학기술정보연구원
{ksyu, livezone, yh.kim086}@kisti.re.kr

# Perform the Analysis for Quantum-Cryptography establishment & response strategies by each domestic carrier

Ki-sung Yu, Wonhyuk Lee, Yong-hwon Kim

요 약

양자컴퓨팅 기술 발현으로 기존 보안체계 위협에 대응하고자 선도국과 더불어 정부 및 국내 기관들의 대응 전략이 좀 더 가시화 되고 있다. 우리나라의 경우 양자암호 통신 기술 개발과 상용화 추진은 통신 3사를 중심으로 양자특별법안이 통과되고 정부의 디지털 뉴딜에 양자 기술을 포함함으로써 양자암호통신이 한 단계 도약하는 계기가 되었다. 앞으로 이러한 과정에서 국내 시장에 미치는 영향은 매우 커질 수 밖 에 없기에 상용화를 위한 현재의 기술 수준이 양자암호통신의 성능, 안정성, 경제성이 충족 될 필요가 있다. 본 논문에서는 이러한 국내 통신사 중심의 양자암호통신망에 대한 대응 전략 및 성과 등을 국가 연구망을 연계한 실용적인 양자암호통신망 서비스 발전을 위한 방향에 대해 제언하고자 한다.

## Ⅰ. 서 론

기존 컴퓨팅 체계의 보안체계는 오래전부터 계산에 기반한 표준화된 RSA에 기반하고 있다. 그러나 양자물리학 원리를 기반으로 큐비트(Qbit)를 이용한 매우 빠른 계산이 가능한 양자컴퓨팅 체계가 현실적으로 다가옴에 따라 기존 보안체계 무력화가 현실화 되고 있다[1]. 이에 양자암호통신 관련 글로벌 이슈에 맞추어 기술 선점과 상용화에 미국, 독일, 일본, 중국 등 주요 국가들이 주력하고 하고 있는 현재 시점에서 국내에서는 정부정책으로 특별법 제정을 통하여 미래 경쟁력 확보에 주력하고 있다. 이에 국내 주요 역할을 하고 있는 통신 3사(케이티, SKT, LGU+) 활동이 특별법과 더불어 행보를 가속화하고 있다[2]. 이는 통신 3사가 상용화를 앞당길 수 있는 이점이 있다. 드러나 원천기술에 주력하고 있는 외국과는 달리 상용화에 주력하는 과정에서 기술의 성능, 안정성, 경제성 등이 실증되어지는 과정이 좀 더 요구되어진다.

본 연구에서는 통신사별 양자암호통신망 연구개발 활동 고찰을 통해 국내 연구개발 통신기반 구축 서비스 역할을 수행하는 국가 연구망과 연계를 통한 실용적인 양자암호통신망 서비스 발전을 위한 방향에 대해 제언하고자 한다.

## Ⅱ. 본론

본 논문에서의 분석은 국내 통신사들이 정부정책(뉴딜종합계획(2020), 국가전략기술육성방안(2022))을 계기로 그 동안 양자암호통신망 구축과 관련된 대응활동을 보다 강화된 추진전략체계를 갖추고 양자를 이용해 키를 공유하는 양자키분배(QKD,Quantum Key Distribution)[3]와 양자컴퓨팅 환경에서 안전한 암호 알고리즘을 중심으로 하는 양자내성암호(PQC, Post Quantum Cryptography)[4]에 따른 양자암호통신망 구축 및 대응전략으로 구분 되어 진다.

먼저 양자암호통신망을 구축 방향을 목표로 하는 통신사를 보면, SKT는 국내 최초로 양자기술연구소 설립(2011)하고 활동을 시작하였다. 이에 따라 통신망구축은 세계최초로 지역간(대전-세종) 양자암호통신기술 적용(2016), 유럽연합(EU) 산하 프로젝트 양자통신회원사 중 가장 많은 구간의 시험망을 구축(2019), 정부정책에 따른 9개 구간 시험망 구축(2021)을 하였으며, 향후 전국 주요 도시간 연동을 통해 다양한 분야에 서비스를 지향하는 양자암호 하이웨이 구축을 목표로 하고 있다. 또한 이를 위해 양자암호통신 기술 강화(IDQ인수, 2018)를 통한 QKD, QRNG, Q-Sensing 기술 연구개발에 주력하고 있다.

KT의 추진방향은 양자암호통신의 표준화를 통한 기술개방으로 시장 선도를 통한 활성화에 주력하고 있다. 이러한 전략은 국제 표준화를 연계한 양자키분배(QKD) 성능평가 기준을 국제전기통신연합(ITU)으로부터 세계최초로 국제표준화받기도 하였으며, “양자암호통신 네트워크 구조, 양자암호통신 네트워크 관리,를 위한 기능 요구사항, 양자암호통신 네트워크의 제어 및 관리기술” 3건의 표준화를 ITU로부터 승인 받았다. 또한 “양자암호통신 네트워크의 서비스품질 파라미터와 양자암호통신 네트워크 비즈니스 모델” 부문도 표준화 제정을 추진하고 있다.

표준화에 이어 양자키분배(QKD) 기반한 양자암호통신기술 개발에도 주력하고 있다. 순수 국산기술을 통해 고속양자암호키분배시스템구현(20kbps;4,000노드 연동수준), 양자암호키분배 전용어뎁터 개발, 소프트웨어기반 자동화 솔루션(Q-SDN, Quantum-Software Defined Network) 개발, 양자하이브리드“ 개발 등 양자암호통신 장비 및 소프트웨어 개발에 주력하고 있다.

LGU+의 다른 통신사와는 달리 양자내성암호(PQC)가 적용된 전송 장비를 통해 양자암호 통신망을 구현하는 전략을 중심으로 추진하고 있다. PQC 소프트웨어적인 특성으로 인해 현재 미국국립표준기술연구소(NIST) 주도로 IBM, 아마존, 구글, MS 등 글로벌 기업들과 표준화 작업을 진행하고 있다. 또한 관련 다수의 기업과 연구소 연합으로 이루어진 ”OQSP; Spen Quantum Safe Project“를 통해 지속적 연구개발이 추진되고 있다.

LGU+는 광전송장비에 장착되는 PQC 암호화모듈을 세계최초로 개발(2022), 국내 최초 IoT 단말용 양자보안칩 개발(2020), 국내 최초로 IoT

단말용 양자 보안 칩 개발이 대표적이다.

양자암호통신 관련 국내 통신사들의 상용화 방향은 SKT의 양자암호키 분배, 양자난수생성기, 양자센싱으로 사업화 하고 있다. 또한 글로벌데이터센터 기업과 연계한 “서비스형 QKD” 추진을 통한 기업용 구독 모델 서비스로의 확대를 꾀하고 있다. 이밖에도 QRNG 칩을 통한 다양한 분야에 보안 인증서비스 사업 등을 확대하고 있다. KT는 양자암호전용회선 서비스 출시를 통해 상용화를 추진하고 있다. 이러한 것은 정부의 양자암호통신망 구축·운영 사업자 선정을 통한 지역간 양자암호통신망 구축 등 지역간 양자암호통신망 구축을 통하여 타 사보다 양자암호전용회선 서비스 상용화에 주력하고 있다. LGU+는 PQC암호화 모듈 및 양자보안 칩을 통한 데이터전송의 전 계층과 국내외 각기 다른 네트워크 구조 및 다양한 비대면 서비스 등으로 주력하고 있다[5].

양자암호통신의 현실화는 통신기반과 보안기술의 신뢰성을 전제로 할 때 가능하기에 산·학·연 들이 각자의 역할에 맞추어 연구개발을 추진하고 정부 주도의 정책은 미래 대응을 위한 현실과제로의 인식이 자리 잡고 있기 때문이다. 과거 새로운 기술의 출현에서 시장으로의 전환 과정에서 알 수 있듯이 관건은 이용자들의 신뢰성을 제공할 수 있는 실증이 다양하게 제공되어야 한다. 이러한 문제를 해소할 있는 것은 그 동안 객관적으로 기술 연구·개발을 통해 인프라-이용자-서비스 체계를 갖추고 있는 국가 연구망을 활용하는 것이다. 공공 성격의 연구망은 현재 양자암호통신과 연계되어지는 양자네트워킹 기반 및 구현 기술을 추진하고 있다. 빠른 상용화 단계를 위해서는 통신사의 장점과 국가 연구망의 장점을 융합할 수 있는 인프라·기술 추진체계를 구축하여 양자암호통신망 조기 구현할 수 있는 방안을 제안하고자 한다.

## Ⅲ. 결론

본 논문에서는 양자암호통신의 기술증진과 상용화와 관련된 국내 통신사들의 인프라 구축 및 대응전략 등의 분석을 실시하였으며, 조기에 시장의 활성화와 안정화를 위한 방안을 제안하였다. 이를 통하여 미래 양자암호통신망 서비스 환경 구축에 기여 할 수 있기를 기대한다.

## ACKNOWLEDGMENT

본 연구는 2023년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다.

## 참 고 문 헌

[1] Cao, Yuan, et al. "The evolution of quantum key distribution networks: On the road to the qinternet." IEEE Communications Surveys & Tutorials 24.2 (2022): 839-894.

[2] 과학기술정보통신부(2021), 양자산업 생태계 활성화를 위한 양자암호통신 시범사업 본격 착수.

[3] Scarani, Valerio, et al. "The security of practical quantum key distribution." Reviews of modern physics 81.3 (2009): 1301.

[4] Bernstein, Daniel J., and Tanja Lange. "Post-quantum cryptography." Nature 549.7671 (2017): 188-194.

[5] 문병도(2022.01.26)이통 3사, 양자암호 앞으로…SKT '인프라가 구축'·KT '글로벌 표준 인증'·LG U+ '공공·민간분야에 검증'.