

양자 정보 통신 기술 표준화 동향 연구

김세진

한국정보통신기술협회

sejin7120@tta.or.kr

A Study on the standardization trends of Quantum Information Communication Technology

Kim Se Jin

Telecommunication Technology Association.

요 약

양자 정보 통신 기술은 양자키분배, 양자 암호, 양자 컴퓨팅 분야에서 집중적으로 개발되어 위성 양자암호통신, 양자 컴퓨팅 기계학습 개발 등 융합분야로 확장되고 있는 추세다. 본 논문에서는 국제전기통신연합(ITU)과 ISO/IEC의 합동기술위원회(JTC 1)를 비롯하여 유럽전기통신표준협회(ETSI)에서 다루는 양자 정보 통신 기술 분야의 표준화 동향을 살펴보고, 이에 따른 향후 방향성을 제시하고자 한다.

I. 서론

양자(Quantum)란 물리학에서 상호작용과 관련된 모든 독립체(에너지)의 최소 단위(광자, 전자, 양성자, 중성자 등)이며, 미시적 관점에서 일어나는 양자만의 특성(양자상태)을 기존 ICT기술에 활용한 분야가 양자 정보 통신 기술이다. 즉, 중첩성, 불확정성, 얽힘, 비가역성이라는 양자상태를 생성, 제정, 측정 및 분석하는 기술이며 크게 양자통신, 양자컴퓨팅, 양자센서/이미징 분야로 나눌 수 있다.[1]

여러 글로벌 IT기업과 많은 나라에서 국가적 차원의 양자 정보 통신 기술 개발이 심화되고 있다. 특히 IBM, 구글, MS, 인텔 등에서 양자 컴퓨팅 기술을 주도하고 있으며, 중국은 위성으로 서울-도쿄 거리의 양자암호통신을 양방향 송수신 성공하였다. 최근에는 양자컴퓨터에서 AI를 구현하는 등 다양한 분야의 융합기술로 확장됨에 따라 많은 국제 표준화기구에서의 표준 개발도 활발해지고 있다. 본 논문에서는 양자 정보 통신 분야의 기술 및 시장 확장에 따른 국제 표준화기구들의 표준화 동향을 다루고자 한다.

II. 본론

ITU에서는 ITU-T SG13(미래네트워크)와 SG17(사이버보안) 연구반에서 활발히 양자 정보 기술 분야의 표준을 개발 중이며 양자정보기술 포커스그룹(QIT4N)을 '19년 9월 신설해 양자암호 응용기술 및 유스케이스 분석 등 ITU-T내 여러 SG간, 타 표준화기구간 상호협력에 주력하고 있다. 국내 통신 3사를 비롯하여 ETRI, KAIST 등 여러 산학연이 상기 그룹들에 참여하고 있으며 특히 SG13에서는 KT와 KAIST, SG17에서는 SKT에서 주도적으로 표준화 추진중이다. 현재까지 SG13에서 권고안 Y.3800과 Y.3801, SG17에서 X.1702와 TR.sec.qkd는 승인되었다.[2]

No.	권고 명 (Work Item)
1	General Aspects of QoS on the Quantum Key Distribution Network (Y.QKDN_qos-gen)
2	Requirements for QoS Assurance of the Quantum Key Distribution Network (Y.QKDN_qos-req)
3	Software Defined Network Control for Quantum Key Distribution Networks (Y.QKDN_SDNC)

4	Functional architecture of the Quantum Key Distribution network (Y.QKDN_Arch)
5	Business role-based models in Quantum Key Distribution Network (Y.QKDN_BM)
6	Key management for Quantum Key Distribution network (Y.QKDN_KM)
7	Control and Management for Quantum Key Distribution Networks (Y.QKDN_CM)
8	Standardization roadmap on trustworthy networking and services including quantum enhanced networks (Y.supp.trust-roadmap)

<SG13에서 진행 중인 양자통신분야 표준화 과제>

상기 표는 승인된 권고안 Y.3800과 Y.3801이외의 SG13에서 진행 중인 양자통신 분야 표준화 과제 목록으로 한국(KT, ETRI, KAIST, LGU+ 등)은 총 8개 중 6개의 에디터로 적극 참여하고 있으며, 중국과 일본 등이 함께 개발 중이다.

No.	권고명(Work Item)
1	Use of cryptographic functions on a key generated in quantum key distribution networks
2	Security requirements for quantum key distribution networks - key management
3	Security requirements for quantum key distribution networks - overview
4	Security requirements for quantum key distribution networks - trusted node
5	Security guidelines for applying quantum-safe algorithms in 5G systems

<SG17에서 진행 중인 양자통신분야 표준화 과제>

상기 표는 승인된 권고안 X.1702와 TR.sec-qkd이외의 SG17에서 진행 중인 양자통신 분야 표준화 과제 목록으로 한국(SKT)이 5개중 3개의 에디터로 SKT의 자회사인 IDQ(스위스), 중국, 일본에서 개발 중이다. 최근 ITU-T에 신설된 양자정보기술 포커스그룹(QIT4N)에서도 KT와 SKT에서 부의장직을 수입, 양자키분배네트워크(QKDN)의 유스케이스 표준 개발에 참여하는 등 한국은 국제 표준화 활동에 발맞춰가고 있다.

과제 번호	제 목
ISO/IEC 23837-1	Information technology security techniques - Security requirements, test and evaluation methods for quantum key distribution - Part 1: Requirements
ISO/IEC 23837-2	Information technology security techniques - Security requirements, test and evaluation methods for quantum key distribution - Part 2: Evaluation and testing methods

<JTC 1/SC 27/WG3에서 진행 중인 양자통신 분야 표준화과제>

상기 표와 같이 JTC 1에서는 정보보안, 사이버보안 및 프라이버시보호 위원회(SC 27)의 보안평가기준, CC분야 작업반(WG3)에서 양자키분배 관련 표준인 ISO/IEC 23837-1, 23837-2를 개발 중에 있다. 두 과제 모두 중국과 영국이 Project Leader로 2022년 제정을 목표로 하고 있다.

올해 6월엔, JTC 1 산하 양자컴퓨팅 분야의 작업반(WG14)이 중국 주도 하에 신설되었다.[3] 미국, 일본, 중국, 영국 및 캐나다의 산학연에서 WG14에서 활동하고 있으며, 표준화과제 WD 4879를 개발하고 있다. 한국은 JTC 1의 여러 위원회의 정회원으로 활동 중이나, 양자 정보 기술 분야의 참여는 저조한 편이었고 최근 들어 SC 27/WG 3 중심으로 점점 활동을 넓혀가고 있다.

유럽전기통신표준협회(ETSI)에서도 2010년부터 양자키분배 모듈, 유스 케이스 및 응용 인터페이스 등 현재까지 9개 표준을 제정, 3건 개정 및 5건을 개발하고 있다. ETSI에 한국의 삼성, LG 등 제조사 및 대구대학교, 한양대학교, ETRI, KETI 등이 멤버로 참여하고 있다. 그러나 표준화기구의 특성상 유럽 통신사, 장비제조사의 주도로 양자 정보 통신 분야 표준화가 이뤄지고 있는 추세다.

III. 결론

본 논문에서는 국내외 양자 정보 기술 표준화 동향에 대해 살펴보았다. 양자 정보 기술은 국제적으로 실질적인 상용화를 위하여 표준화도 기반을 구축하는 단계다. 유럽, 미국, 일본, 최근 양자정보통신 기술의 강자로 주목받는 중국을 비롯하여 많은 나라에서 정책적, 기술적 지원을 강화하고 있다. 우리나라도 양자HCT 핵심기술개발과 종합계획 수립을 통해 양자 ICT 생태계 구축을 추진하고 있다. 올해 양자정보 연구지원센터 출범을 추진하고 있으며 3월 국회 상임위원회를 통과한 ICT특별법 일부 개정 법률안에 ‘양자응용기술’ 및 ‘양자응용산업클러스터’를 도입하는 등 국내 관련 현행법령을 발전시키기 위한 노력을 하고 있다. 또한 ITU, JTC 1 등 여러 표준화기구에서도 양자 정보 통신 기술 표준화 논의에 적극 참여하여 우리나라의 표준 주도권을 잡기 위한 활동 중이다.

ACKNOWLEDGMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2017-0-00063, 국제표준(ISO/IEC) 대응체계 구축 및 국가표준 개발)

참 고 문 헌

- [1] ICT R&D 기술로드맵 2023 미래통신전파 pp.102-104.
- [2] ITU-T SG13(<http://www.itu.int/en/ITU-T/studygroups/2013-2016/13/Pages/default.aspx>)
- [3] ISO-IEC JTC1_N14842_Resolutions.