양자정보통신 기술 국내외 표준화 동향 및 전망

김세진, 이강해*
한국정보통신기술협회
sejin7120@tta.or.kr, kanghae@tta.or.kr*

The standardization trends and prospects of Quantum Information Communication Technology

Kim Se Jin, Lee Kang Hae*
Telecommunication Technology Association

요 약

양자정보통신 기술은 크게 양자암호통신, 양자컴퓨팅 및 양자센서/이미징 분야로 나눌 수 있다. 미국, 유럽, 중국 등 여러 나라에서 양자정보통신 기술의 세부 분야를 심도있게 연구하고 있으며, 양자정보통신 기술의 표준화 주도권을 잡기 위한 경쟁 중이다. 우리나라에서도 양자암호통신 인프라 시범구축 등 양자암호통신 산업 생태계 활성화에 박차를 가하고 있다. 본 논문은 최근 국내외 표준화기구에서 추진되고 있는 양자정보통신 표준화 동향과 향후 전망을 알아본다.

Ⅰ. 서 론

양자정보통신 기술은 ICT기술에 양자역학적 특성을 생성, 제어, 분석하는 기술이다. 중첩성, 불확정성, 얽힘, 비가역성이라는 양자상태를 활용하여 양자암호통신, 양자컴퓨팅, 양자센서/이미징 기술 분야로 나눌 수 있다.[1]

양자정보통신 기술은 1900년대 말 처음으로 양자컴퓨터의 가능성이 언급된 후 전 세계적으로 본격적인 연구가 시작되었다. 양자광소자, 물리량 측정 양자센서, 양자네트워크 등을 활용하여 미래 융합 기술로 주목받고 있으나, 표준화 진행은 개념 및 기반 표준을 개발하는 초기 단계다.

미국, 유럽과 중국 등은 양자정보통신 분야의 주도권을 갖기 위해 적극적으로 정책과 산업을 추진하고 있다. 우리나라에서도 양자암호통신 인프라 시범구축 사업 추진, 양자사업 클러스터 조성 등 양자암호통신 산업 생태계를 구축하고자 노력하고 있다. 이러한 일환으로 우리나라는 국제 표준화기구에서 양자암호통신 표준화에 주도적으로 활동 중에 있다.

본 논문에서는 양자정보통신의 표준화 요소와 여러 표준화기구에서 추진 중인 표준화 동향을 다룬다.

Ⅱ. 본론

양자정보통신 표준화 공통 요소로는 기술 및 시스템에서 사용되는 전반적인 용어와 개념, 시스템 및 서비스 구현에 필요한 정의, 프레임워크, 참조구조, 요구사항, 활용사례 등과 같은 기반 표준이 있다. 현재까지는 양자정보통신 표준화는 양자암호 분야의 기반 표준 구축과 양자컴퓨팅 분야의 용어정의가 이루어지고 있다.

공식표준화기구인 ITU-T에서는 미래인터넷 연구반(SG13)과 정보보호 연구반(SG17)에서 주로 표준을 개발하고 있다. 표준화 개발에 참여하는 국가로는 미국, 중국, 러시아, 스위스 등과 함께 우리나라에서도 통신3사를 비롯하여 ETRI와 순천향대학교 등 다양한 산학연에서 참여 중이다.

SG13연구반에서는 양자암호망의 운용을 위한 키관리, 양자키분배 노드간 연동을 위한 참조모델, 기능요소, 운영절차 등을 표준화 추진 중이며 현재까지 7건 최종승인(오류정정서 2건 포함, 한국 주도 4건) 및 8건 개발(한국 주도 6건) 중이다. 표 1에서 No.1, 3, 4, 7이 KT, ETRI에서 주도로 제정한 권고안이며, 표 2에서 No.5, 7을 제외한 6건 권고안은 KT, ETRI, KAIST 주도로 개발 중에 있다.[2]

<표 1. ITU-T SG13 양자암호통신분야 제정된 권고안>

No.	권고안 명	에디터
1	Y.3800, Overview on networks supporting quantum key distribution	**KT,** 일본
2	Y.3800 Cor.1, Overview on networks supporting quantum key distribution	일본, 스위스
3	Y.3801, Functional requirements for quantum key distribution networks	**KT, ETRI,** 중국, 일본
4	Y.3802, Quantum key distribution networks - Functional architecture	**ETRI,** 중국, 일본
5	Y.3802 Cor.1, Quantum key distribution networks - Functional architecture	일본
6	Y.3803, Quantum key distribution networks - Key management	일본, 중국
7	Y.3804, Quantum Key Distribution Networks - Control and Management	**KT, ETRI,** 중국, 일본

<표 2. ITU-T SG13 양자암호통신분야 개발 중인 권고안>

No.	권고안 명	에디터
1	Y.QKDN-qos-fa, Functional architecture of QoS assurance for quantum key distribution networks	**KT, ETRI,** 중국
2	Y.QKDN-qos-gen, General Aspects of QoS (Quality of Service) on the Quantum Key Distribution Network"	**KT, ETRI**
3	Y.QKDN-qos-ml-req, Requirements of machine learning based QoS assurance for quantum key distribution networks	**KT, ETRI,** 중국
4	Y.QKDN-qos-req, Requirements of QoS Assurance for the Quantum Key Distribution Networks	**KT, ETRI** 중국
5	Y.QKDN_SDNC, Quantum Key Distribution Networks - Software Defined Networking Control	중국
6	Y.QKDN_BM, Quantum Key Distribution Networks - Business role-based models	**KT, ETRI KASIT**
7	Y.supp.QKDN-mla, Quantum Key Distribution Networks - Applications of Machine Learning	중국
8	Y.supp.trust-roadmap, Standardization roadmap on Trustworthy Networking and Services including Quantum Enhanced Networks	**KAIST**

SG17 연구반에서는 양자 잡음 기반 난수생성기, 양자키분배 네트워크 보안 프레임워크 등을 표준 개발 중이며 현재까지 6건 최종 승인(오류정정서 1건 포함, 한국 주도 4건), 5건 개발(한국 주도 3건) 중이다. 표 3에서 No.5를 제외한 5건의 권고안은 SKT, 순천향대 주도로 제정하였으며, 표 4에서 No.1, 2, 4는 SKT주도로 개발 중에 있다.[3]

<표 3. ITU-T SG17 양자암호통신분야 제정된 권고안>

No.	권고안 명	에디터
1	TR.sec-qkd, Technical Report: Security considerations for quantum key distribution network	**순천향대**, 스위스
2	X.1702, Quantum noise random number generator architecture	**SKT**, 스위스, 중국
3	X.1710, Security framework for quantum key distribution networks	**SKT**, 스위스, 중국, 일본
4	X.1714, Key combination and confidential key supply for quantum key distribution networks	**SKT**, 스위스, 일본
5	X.1811, Security guidelines for applying quantum-safe algorithms in 5G systems	중국
6	XSTR-SEC-QKD Cor.1, Security considerations for quantum key distribution network - Cor.1	**SKT**, 스위스

<표 4. ITU-T SG17 양자암호통신분야 개발 중인 권고안>

No.	권고안 명	에디터
1	TR.qs-dlt, Technical Report: Guidelines for quantum-safe DLT system	**SKT**, 중국
2	X.1712, Security requirements for quantum key distribution networks - key management	**SKT**, 중국, 일본
3	X.sec_QKDN_AA, Authentication and authorization in QKDN using quantum safe cryptography	일본
4	X.sec_QKDN_CM, Security requirements and measures for quantum key distribution networks - control and management	**ETRI**, 일본
5	X.sec-QKDN-tn, Security requirements and designs for quantum key distribution networks - trusted node	중국

'19년 12월에 양자정보기술 포커스그룹(FG-QIT4N)을 신설하여 양자암호 응용기술 및 유스케이스 분석 등 표준화 진행 중이다. FG-QIT4N에서는 한국에서도 부의장(KT, SKT)을 수임 중이며, 양자정보통신 네트워크 및 양자키정보와 관련한 9건의 기술보고서를 개발(한국 주도 1건) 중에 있다.[4]

공식표준화기구 ISO/IEC/JTC 1에서는 '20년 6월에 JTC 1 직속으로 양자컴퓨팅 작업반(WG 14) 설립[5]되어, 본격적인 표준화 추진을 위한 타 표준화 기구 동향 및 기술 개발 현황 등의 사전조사를 시행 중에 있다. 표준화 개발은 초기단계로 양자컴퓨팅 용어에 대한 표준안 1건을 개발 중이다. 작업반에 참여하는 국가로는 미국, 중국, 한국(ETRI) 등 10여명이 참여하고 있다.

또한 JTC 1 산하 정보보안 위원회(SC 27)의 정보보안 평가기준 작업반(WG 3)에서 양자키분배 보안 요구사항 및 시험 평가에 대한 표준 2건을 추진 중이다.

<표 5. JTC 1/WG14, JTC 1/SC 27/WG3 양자통신분야 개발 중인 표준>

No.	표준안 명	에디터
1	ISO/IEC AWI 4879, Quantum computing — Terminology and vocabulary	중국
2	ISO/IEC CD 23837-1, Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements	중국, 영국
3	ISO/IEC CD 23837-2, Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods	러시아, 중국, 영국

사실표준화기구에서도 양자정보통신 관련 표준화가 진행 중에 있다. IEEE에서는 양자컴퓨팅 성능구조와 양자통신 정의 등에 대한 표준안 프로젝트를 승인하고, 양자표준작업그룹(QOWG)에서 다양한 명칭 및 용어 정의를 개발 중에 있다. ETSI에서는 양자 암호해독, 양자키분배와 같은 표준을 제정 및 개발 중에 있으며, 삼성, KG 등 제조사 및 대구대학교, 한양대학교, ETRI, KETI 등이 ETSI 멤버로 참여하고 있다. 그러나 표준화 기구의 지역 특성상 유럽의 통신사 및 제조사의 주도로 표준화가 이뤄지고 있는 추세다.

국내에서도 미러커미티인 한국ITU연구위원회 연구반, JTC 1 전문위원회와 퀀텀포럼 등에서 양자키분배 네트워크 분야의 표준화를 주도하며 우리나라 산업계에 적용시키기 위한 단체표준을 개발하고 있다.

Ⅲ. 결론

미국(구글, IBM, 인텔 등)과 유럽(도이치텔레콤, 오렌지, 제네바 대학 등)은 양자컴퓨팅, 양자암호통신 분야 기술을 선도하고 있으며, 최근에는 중국에서도 양자통신 위성을 개발하고 2030년까지의 주요 국가간 양자네트워크 시험 계획을 발표하는 등 활발히 추진 중에 있다. 우리나라에서도 정책과 양자 산업 클러스터를 조성하고, 양자정보통신 기술 전담기관(TTA, NIPA, NIA, NRF, RRA 등) 지정하여 양자 ICT핵심기술 개발 및 원천기술 확보를 위한 정책을 추진 중에 있다.[6]

본 논문에서는 ITU-T 표준화기구 중심으로 양자정보통신 표준화를 주도하는 국가와 우리나라에서의 개발 중인 표준 현황을 알아보았다. 양자정보통신 분야의 초기 시장의 선점을 위하여 각 국가의 정부 정책 및 기술개발에 발맞춘 글로벌 표준화 주도권 경쟁은 심화되고 있다. 양자정보통신 표준화는 양자암호통신과 양자컴퓨팅의 기본적인 표준만이 개발된 상태인 만큼, 머지않아 양자센서와 양자광소자 등의 다른 세부 분야의 기반 표준도 다뤄질 것으로 보인다. 향후 개념과 요구사항의 표준화 수준에서 시스템 구조와 상세 구현까지 표준화 성숙도도 깊어질 전망이며, 세부기술별 시스템 및 서비스 표준화에 대하여 정리할 예정이다.

ACKNOWLEDGMENT

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2017-0-00069, 공식표준화기구(ITU/APT등) 표준화대응연구)

참 고 문 헌

[1] ICT R&D 기술로드맵 2025 ICT디바이스·양자 pp. 132-144.

[2] ITU-T SG13(https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.aspx).(2021.05 방문)

[3] ITU-T SG17(https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx).(2021.05 방문)

[4] ITU-T FG-QIT4N(https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx).(2021.05 방문)

[5] ISO-IEC JTC1_N14842_Resolutions.

[6] https://www.etnews.com/20210428000190