

양자 표준화 분야의 국내외 동향 분석 및 고찰

오지연, 김학훈, 차순일

한국정보통신기술협회(TTA)

jiyeon@tta.or.kr, hakhoonk@tta.or.kr, sicha@tta.or.kr

A Proposal & Analysis for Domestic and International Trends in the Field of Quantum Standardization

Ji-Yeon Oh, Hak-Hoon Kim, Soon-Il Cha

Telecommunications Technology Association

요약

본 논문은 양자 고유의 특성(얽힘, 중첩 등)을 활용하여 기존 기술의 한계를 뛰어넘는 초고속연산(양자컴퓨팅), 초신뢰 보안(양자통신), 초정밀 계측(양자센싱) 분야의 국내외 표준화 동향에 대한 방향성 및 시사점에 대하여 살펴본다.

I. 서론

양자(Quantum)는 불연속적인 입자성과 중첩이 가능한 파동성을 동시에 갖는 개체로서 에너지, 운동량 등 불연속적인 물리량 현상 전반을 의미한다[1]. 양자기술은 양자 고유의 특성(얽힘, 중첩 등)을 활용하여 기존 기술의 한계를 뛰어넘는 초고속연산(양자컴퓨팅), 초신뢰 보안(양자통신), 초정밀 계측(양자센싱)을 가능케 하는 파괴적 혁신 기술로, 세계적으로 큰 주목을 받고 있으며, 정부는 2022년 ‘양자암호통신 시범인프라 구축사업’을 통하여 공공·의료·산업 분야에 서비스 발굴 및 기반을 마련하였다[2].

양자기술은 양자통신, 양자센서, 양자컴퓨터 등 크게 3가지 분야로 나눌 수 있다. 이들 분야 중에는 기존 표준화 기구에서 세부 분야별로 표준화 위원회를 통해 10여 년 이상 표준화를 진행한 곳도 있으며 이제 막 표준화를 시작하고 있는 곳도 있다. 이는 양자기술이 더 이상 꿈의 기술이 아니고 현실의 기술이며 초기시장을 형성하기 시작했다는 의미이며, 이에 따른 표준화 요구가 증대되고 있음을 말한다[3].

현재 보편화가 완료된 양자기술은 대부분 하드웨어에 치중되어 있어 하드웨어에 적용될 소프트웨어의 기술이 개발되고 있다. 따라서 시의적절한 표준 제정을 통해 기술의 발전 속도를 높이고 완성도와 안전성을 높인다면 양자기술의 보편화가 한층 빨라질 것이다[7].

또한, 양자기술은 큐비트의 비안전성으로 인하여 오류가 발생하는 문제가 있기 때문에 높은 수준의 오류 복구 기술이 필요하다는 공통 분모가 있다. 따라서 관련 표준 관점에서 보면 양자의 오류 복구에 가장 강점이 있는 기술이 표준으로 채택될 가능성이 높다[1].

본 연구에서는 표준화 초기 단계인 양자기술 분야에서 국제표준 선점을 통하여 양자 기술을 선도하기 위해 우리나라 양자기술 분야가 나아갈 방향성을 제시하고자 한다.



[그림 1] 대한민국 양자과학 기술 비전과 정책목표

(출처: 대한민국 양자과학기술 비전 2023.6)

II. 관련 국내외 동향

과학기술정보통신부의 2023년 발간된 양자정보기술 백서에 의하면 전 세계 양자기술 시장의 총규모는 25조 9,024억 원으로 보고 되고 있다[4]. 연평균 29.2%의 높은 성장률을 지속하고 있으며 2030년에는 155조 5,112억 원으로 커질 것으로 예측 되고 있다[4]. 우리나라의 경우 다른 나라에 비해 출발이 늦은 탓에 큰 기술격차를 보이고 있다. 이에 과학기술정보통신부에서는 2019년부터 양자센서·양자컴퓨터·양자암호통신 분야 신규 사업 지원을 확대하고 있다. 대학, 연구소 등 연구조직을 강화하고, 양자암호통신인프라 시범사업을 추진 중이며 산업 생태계 활성화를 위한 다양한 노력도 기울이고 있다[4].

이에, 우리나라는 지난 6월 정부가 발표한 ‘대한민국 양자과학기술전략’ 계획에 의거하여 2035년까지 민·관 합동으로 3조 원을 투자하여 선도국 대비 85% 기술 수준에 도달하는 것을 목표로 삼고 있다[1].

<표 1> 국내외 양자기술 표준화기구별 표준화 내용

SDO		표준화 내용	
국외	ISO/IEC	JTC 3	• 양자기술 표준화(2024년 신설)
		JTC 1 SC 27	• 양자 암호통신 관련 SC 표준을 추진
		JTC 1 WG 14	• 양자컴퓨팅 용어 표준화(JTC 3으로 통합예정)
	ITU-T	SG 13	• QKDN 요구사항, 구조, 키 관리, 운영관리 기술, SDN 적용방안, 비즈니스 모델 및 서비스 품질
		SG 17	• 양자암호 기술, 통신망에서 양자 키 분배 기술을 위한 보안 프레임워크, 양자 노이즈 난수 생성기 구조 등의 핵심기술 • QKDN 환경에 적용될 보안 요구사항 및 상세 보안기술
		FG-QIT4N	• 네트워크를 위한 양자 정보기술 선행 표준화를 위한 기술 분석
	ETSI	QKD ISG	• QKD 모듈 보안 표준 제정으로 양자 키 분배망의 시험절차 및 인증규격 표준화 • 표준화를 통해 보안성 증명
	IEEE	P1913	• 소프트웨어 정의 양자통신에 대한 표준화 진행
		P2995	• 양자 알고리즘 설계 및 개발
		P7130	• 양자컴퓨터 용어 정의
P7131		• 양자컴퓨터 성능측정방법	
TTA	TC 2	• QKD 표준화(통신 관점)	
	TC 5	• QKD 표준화(보안 관점)	
국내	KETI, KIMM	IEC SEG 14 IEC/ISO JTC 3	• 양자기술 국문백서(2020년 12월), 양자기술 영문백서(2021년 10월) 발간 • 양자기술 전문위원회 운영(2022년 8월 신설) : IEC SEG 14와 IEC/ISO JTC 3 대응 위원회 구성 운영, 양자기술 표준화 로드맵 구축(11개 표준화 아이템 발굴), 양자기술 표준포럼 출범 운영(2023년 11월) 등 수행

(출처: 국가기술표준원 표준이슈포커스 2024.3)

III. 양자기술 관련 표준화

양자컴퓨팅은 최적화, 암호해독, 시뮬레이션과 같은 대량의 데이터 또는 복잡한 계산에 있어 기존 컴퓨터보다 훨씬 빠른 처리가 가능하며, 양자통신은 암호기를 포함하는 단일 광자(photon)를 전송하는 방식으로, 광자 측정을 이용한 암호키와 관련된 암호통신을 말한다[5]. 양자센싱은 양자가 자기장, 전기장, 중력 등에 매우 민감한 특성을 활용하여 기존 센싱/계측 기술보다 정밀하고 광범위한 측정이 가능한 기술을 의미한다[5]. 에너지의 최소 단위인 양자의 물리적 특성(양자중첩, 양자얽힘, 불확정성 등)을 이용한 차세대 정보기술로 초고속 대용량 연산 및 암호통신이 가능한 기술에 대한 기술 개발 및 선도적인 국제 및 국내 표준에 대한 대비가 시급한 실정이다.

또한, 양자통신은 기술 발전 단계별로 양자키분배(QKD)-양자키분배네트워크(QKDN)-양자키분배네트워크 연동(QKDNi)-양자인터넷(QI)과 같이 구분할 수 있으며, 양자키분배는 송신자와 수신자 사이에서 양자채널을 통해 큐비트를 전달하는 QKD 시스템을 이용하여 양자 암호키를 생성·전달하는 기술이다. 양자키분배네트워크는 QKD 시스템의 한계를 극복하여 장 거리에 있는 다수에게 암호키를 전달할 수 있도록 확장한 기술을 말하며, 양자키분배네트워크 연동은 양자키분배네트워크 사업자 간 연동을 지원하는 기술로서 이를 통해 사업자가 다른 고객 간에도 양자암호통신이 가능하다. 또한, 양자키분배의 규격 및 시험 표준, 시스템 표준, 프로토콜 및 키관리 표준, 네트워크 및 망 관리 표준, 양자 컴퓨팅 용어의 표준과 양자네트워크의 구조 표준이 요구된다[6].

한편, 양자네트워크는 사용자 데이터 같은 대용량 정보를 고속의 큐비트로 전송하는 기술로서 양자 메모리, 양자 리피터 등의 핵심 요소를 포함한다. 양자인터넷은 양자네트워크 간의 통신을 지원하는 연동 기술로서 양자통신이 전 세계에 가능하도록 한다.

현재까지 표준화 연구는 양자키분배네트워크 표준과 연동 표준 위주로 진행되었으나, 향후 양자네트워크의 신규 연구가 진행되고 있으며, 이러한 연구를 기반으로 양자네트워크 표준화 작업이 활발히 진행될 전망이다[1].

IV. 결론

미국, 유럽, 중국 등 세계 주요국들은 양자통신, 양자컴퓨팅 등 기술개발 및 관련 기초과학 연구 부문에 국가적 투자를 지속하고 있다. 이와 관련하여 미래 기술 혁신을 선도할 양자기술의 국제표준화 위원회가 한국과 영국 주도로 신설되었으며, 우리나라가 초대 의장을 배출하였다[5].

즉 우리나라가 세기의 화두인 양자기술의 표준 제정을 주도하게 된 것이다. 4차 산업혁명 시대에서는 표준이 곧 기업과 국가의 경쟁력과 직결되기 때문에 이를 선점하려는 각국의 경쟁이 치열하다.

현재 우리나라 양자기술력은 세계10위권 이내로 평가받는다. 세계 어느 나라도 양자기술의 보편적인 활용에는 성공하지 못했기 때문에 선제적인 표준제정으로 기술의 활용성을 높이고 시장을 선점함으로써 해당 산업의 주도권을 확보해야 한다[6].

TTA PG225(양자통신)는 현재 양자통신 위주의 표준화 활동에 머물러 있다. 하지만 가까운 미래에 양자컴퓨팅과 양자센싱은 양자통신을 이용하는 단골 고객이 될 것이다. 양자통신은 고객이 충분히 만족할 만한 좋은 서비스를 제공하기 위하여 고객의 요구사항을 이해하고 해결책을 제시할 수 있어야 할 것이다. 이러한 관점에서 TTA PG225는 양자컴퓨팅과 양자센싱의 표준화가 활성화되도록 인큐베이터 역할도 담당할 수 있을 것이다[2].

또한 국제 표준화 무대에서의 선제적 활동을 위한 차세대 공략, 선도경쟁 공략, 추격/협력 공략, 지속/확산 공략, 전략적 수용 관련 국제표준화 전략 연구가 필요할 것으로 사료된다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2022-0-00007, ICT국내표준화연구)

참고 문헌

- [1] 김정윤(2023). ICT전문가인터뷰. *양자로 다시 쓰는 ICT*. 2023(2010), 8-13.
- [2] 김정윤(2023). 양자로 다시 쓰는 ICT. *양자로 다시 쓰는 ICT*. 2023(2010), 6-7.
- [3] 박성수(2023). 양자기술개발 지원정책의 방향성과 로드맵. *양자로 다시 쓰는 ICT*. 2023(2010), 36-42.
- [4] 과학기술정보통신부(2023). *양자정보기술 백서*. 2023, 31-54
- [6] 국가기술표준원(2024). *표준이슈포커스*. 2024(2), 7-16.
- [5] 국가기술표준원(2024, 2월 22일). 21세기 최초 설립된 '양자기술 국제표준화 공동기술위원회' 초대 의장으로 한국인 선출 [보도자료]. 다음에서 검색됨 <https://www.kats.go.kr/mobile/content.do?cmsid=482&skin=/mobile/&mode=view&page=&cid=24322>
- [6] 국가기술표준원(2024). *표준이슈포커스*. 2024(2), 7-16.