편집위원 : 박성수(ETRI)

양자기술관련 국제표준화 동향

박준식(공동교신저자), 황태호(공동교신저자), 주정진*, 이택민**, 한지수
한국전자기술연구원, 한국전자통신연구원*, 한국기계연구원**

요 약

양자기술은 기존 기술의 한계를 극복하기 위한 유망한 미래 기술 중 하나로 주요 선진국을 중심으로 연구개발이 활발하게 이루어지고 있다. 이러한 상황에서 양자기술에 대한 국가간의 표준화 경쟁은 점차 심화될 것으로 예상된다. 따라서, 본 원고에서는 양자기술에 대한 세계적인 공적 또는 사실상 표준화 동향을 파악함으로써 우리나라의 양자기술 국제표준화 분야에서의 위치를 확인하고, 향후 양자기술 표준화에 대한 전략 수립에 도움이 되고자 한다. 양자기술은 다양한 응용분야가 있으나, 크게 양자컴퓨팅, 양자통신, 양자센싱 분야로 나눌 수 있다. 그러나, 양자센싱 분야는 실제 국제 표준화 활동이 다른 두 분야에 비해 활발하지 않아 양자컴퓨팅과 양자통신과 관련된 국제표준화 동향을 중심으로 알아보았다. 그 중에서 ISO/IEC JTC1 (정보기술) WG14 (양자컴퓨팅) 에서는 2020년부터 양자컴퓨팅 관련 표준화를 시작하여 현재 용어 정의와 어휘에 대한 표준화 (ISO/IEC WD 4879, Quantum computing - Terminology and vocabulary)를 추진하고 있다. 양자기술에서는 양자통신, 양자컴퓨팅, 양자센싱 등 다양한 분야를 다루기 때문에 기존에 존재하는 기술위원회 (Technical Committee)와 중복이 되지 않거나 최소화하는 방향에서 ISO/IEC JTC1이나 IEC 등의 공적표준화 기구 안에서 양자기술 (Quantum Technology) 관련 기술위원회 (Technical Committee) 제안과 설립을 추진한다면, 양자기술 분야 국제표준화에 있어서 우리나라가 주도적인 역할을 할 수 있을 것으로 사료된다.

Ⅰ. 서 론

국제표준화의 공적기구는 1947년에 설립된 지적, 과학, 기술, 경제 등 일반 분야의 국제표준 제정, 보급을 하고 있는 ISO (International Organization for Standardization), 1906년에 설립되어 전기전자 분야의 국제표준 제정, 보급을 맡고 있는 IEC (International Electrotechnical Commission), 그리고, 1865년에 설립되어 유무선 통신, 전파, 방송, 위성주파수 등에 대한 기술기준 및 표준의 개발, 보급과 국제협력 수행을 하고 있는 ITU (International Telecommunication Union) 등이 있다[1]. IEC나 ISO의 경우 규범적 성격의 공적표준을 다룬다는 점이 있으나, IS (International Standard) 기준으로 보았을 때 국제표준 제안에서 제정까지 대략적으로 6단계를 거쳐야 하기 때문에 약 3년 이내의 비교적 긴 시간이 소요된다. 여기서 6단계는 예비단계 (PWI, Preliminary Work Item), 제안단계 (NWIP, New Work Item Proposal), 준비단계 (WD, Working Draft), 위원회 단계 (CD, Committee Draft), 질의단계 (ISO의 경우 DIS (Draft International Standard), IEC의 경우 CDV(Committee Draft for Vote)), 승인단계 (FDIS, Final Draft International Standard), 그리고, 출판단계(IS, International Standard)로 구성된다[1]. IEC와 ISO에는 IS 하위 규격이라고 할 수 있는 TS (Technical Specification)와 TR(Technical Reports) 규격이 있으며, CD 단계 후 바로 DTS (Draft TS) 또는 DTR (Draft TR)단계로 넘어가서 투표 후 발간하게 되므로, IS보다 제안에서 발간까지의 시간이 상대적으로 짧게 된다[2].

사실상 표준화 기구는 IEEE(Institute of Electrical and Electronics Engineers), JEDEC (Solid State Technology Association) 등 다양하다. 사실상 표준화 기구를 통한 표준 제정은 일반적으로 1년 이내에 진행되어 공적표준화 기구의 표준에 소요되는 시간보다 짧기 때문에 기술발전 속도가 빠른 분야의 경우 신속하게 표준을 선점할 수 있다는 유리한 면이 있다.

양자기술 관련 표준화 활동은 위의 표준화 기구 중에서 공적표준화 기구인ISO, IEC, ITU-T (ITU중 전기통신분야의 Sector), 그리고, 사실상 표준화 기구인 IEEE 등에서 진행되고 있는 것으로 파악된다. 한편, 한국산업표준 (KS: Korean Industrial Standards)은 산업표준화법에 의거하여 산업표준심의회의 심의를 거쳐 국가기술표준원장이 고시함으로써 확정되는 국가표준으로서 약칭하여 KS로 표시하는데[3], 우리나라 내부에서 필요한 기술을 제안하여 KS표준 또는 규격을 제정하기도 하지만, 위

에서 언급한 공적표준화 기구에서 발간된 국제표준들의 부합화(번역) 과정을 통해 KS 표준이 제정되는 경우도 많은 편이다. 표준이라는 표현과 규격이라는 표현은 자주 혼용되어 사용된다.

양자기술 국제표준화 활동은 공적표준화 기구와 사실상 표준화 기구들에서 최근 활발하게 진행되고 있다. 양자기술 국제표준화 분야는 아래 크게 양자컴퓨팅, 양자통신, 양자센싱 분야로 나눌 수 있다. 그런데, 양자센싱 분야는 양자컴퓨팅과 양자통신 분야에 비하여 상대적으로 국제표준화 활동이 활발하지 않은 편이기 때문에 본 원고에서는 자세히 다루지 않게 되었다. 따라서, 양자컴퓨팅과 양자통신 분야의 국제표준화 활동에 대하여 주로 기술하였다.

Ⅱ. 본 론

양자기술 국제표준화 관련 공적 표준화 기구와 사실상 표준화 기구를 간략하게 요약하면 〈그림 1〉과 〈표 1〉에서와 같다. ISO/IEC JTC1 WG14에서는 양자컴퓨팅 기술에 대하여 중국 주도로 해당 기술 정의 등의 작업이 시작되었다[2][4]. ISO/IEC JTC1 SC27에서는 보안 기술 관련하여 study group이 시작되었다. ISO/IEC JTC1 SC7에서는 소프트웨어시스템과 시스템 공학이라는 주제로 양자암호화 관련 학습 기관을 운영 중이다[2][4]. 유럽전기통신표준협회 (ETSI)에서는 양자암호화 관련 20개의 그룹 규격을 제정하였다[5]. ITU-T에서는 SG13과 SG17에서 양자키 분배 시스템으로 실제 네트워크를 구성하고 사용하는 부분에 있어서 필요한 부분을 중심으로 표준화를 진행해 나가고 있다[6]. 그러나, 양자센서 분야에서는 공적 또는 사실상 표준화 활동이 상대적으로 활발하지 않은 것으로 보인다.

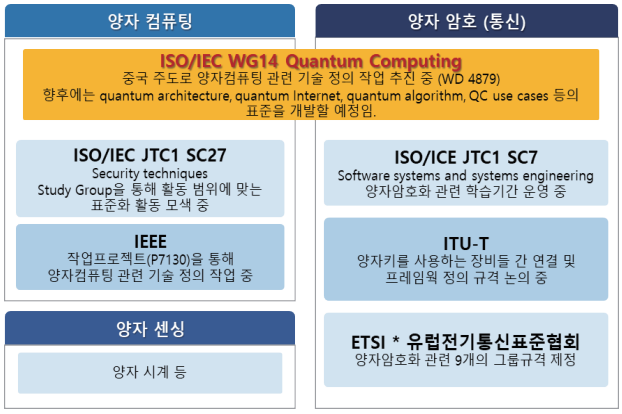

그림 1. 양자기술 국제표준화 관련 공적 표준화 기구와 사실상 표준화 기구 [2], [4]-[7]

표 1. 양자기술 국제표준화 관련 공적 표준화 기구와 사실상 표준화 기구와 활동 내용 요약

출처: [2], [4]-[9]

구분	단체명	작업 그룹 명칭	표준화 활동 내용
국제	ISO/IEC JTC1 WG14	Quantum Computing	(양자컴퓨팅 전반) 현재 용어와 어휘에 대한 표준(ISO/IEC WD 4879, Quantum computing-Terminology and vocabulary)하나 만을 개발 중 향후 quantum architecture, quantum internet, quantum algorithm, QC use cases 등에 표준을 개발할 예정임.
국제	ISO/IEC JTC1 SC27	Security techniques	(양자암호(양자키 분배)) 요구사항, 시험, 평가방법 등에 대하여 스터디 기간 진행중
국제	ISO/IEC JTC1 SC7	Software systems and systems engineering	(양자컴퓨팅) 스터디그룹을 구성하여 양자컴퓨팅 전반에 대하여 표준포트폴리오 작성 중
국제	IEEE	-	(양자컴퓨팅) 관련된 개념에 대한 정의 작업 중
국제	ITU-T	-	(양자암호) 주제별 표준화활동을 스터디 그룹을 만들어 작업 중이며, 이동통신, 네트워크, IoT 관련 보안의 측면에서 양자컴퓨팅 접근 중
지역	ETSI	ISG QKD_ Quantum Key Distribution	(양자암호) 양자암호 기술 관련 자체 표준 제정
지역	ETSI	TC Cyber WG QSC (현재 활동 종료)	(양자암호) 양자암호 관련 논의 중
지역	NIST	-	(양자암호(양자내성암호) 양자내성암호 관련 연구중
민간	CSA	-	양자암호(양자내성암호) 양자내성암호 관련 연구중

ITU-T, ISO/IEC JTC1, ETSI 등 주요 표준화 기구에서 양자키 분배 (QKD, Quantum Key Distribution)와 관련된 표준을 진행 중이다[6].

ITU-T에서는 SG13 (미래인터넷)과 SG17(보안)에서 양자키 분배 시스템으로 실제 네트워크를 구성하고 사용하는 부분에 있어서 필요한 부분을 중심으로 표준화를 진행해 나가고 있다. SG13에서는 양자키 분배망 프레임워크 연구반 승인(Consent), (SG17)'양자키 분배망 양자키 분배망 네트워크 보안 요구사항 (개요, 키 관리, 암호 기능 사용) 등 신규 아이템 3건이 승인되었다. 한국의 통신사업자들에 의하여 주도적으로 제안된 양자키 분배 네트워크에 대한 표준화가 2018년 9월 ITU-T SG13 회

의에서 착수되었다[6]. 이후 SG13은 SG15(전달, 액세스)를 포함하여 ITU-T 내부 SG(Study Group)들에게 관련 표준 착수를 통보하는 liaison을 송부하였으며, 2018년 10월 개최된 SG15 총회에서는 관련 liaison 문서(Framework for Networks to supporting Quantum Key Distribution)가 Q12/15에서 검토되었다[10]. SG17에서의 양자암호 표준화는 2018년 8월 SG17 회의에서 시작되었다. SK텔레콤 및 IDQ (ID Quantique)에서 제안한 2개의 신규 표준화 과제 (Work Item)에서 시작되었다. 이후 2019년 1월 SG17 회의에서 3개의 추가 신규 표준화 과제가 승인되었다[11].

한편, 국내TTA(한국정보통신기술협회)에서는 ETSI 표준을 그대로 인용하여 국내 영문표준으로 만들었고, 양자키 분배와 관련한 표준 2건도 제정되었다[12][13]. TTA 표준화위원회 산하 광전송(PG201), 정보보호기반(PG501) 프로젝트 그룹에서 양자키분배 관련 표준화가 진행되었다. TC2(통신망), PG201(광전송), TC5(정보보호), PG501(정보보호기반) 등에서 관련 표준 개발을 진행하고 있다[12].

ISO/IEC JTC1의 WG14 (Quantum Computing)에서는 9월에 첫 번째 회의에 이어 11월 9일 JTC1 Plenary 회의가 2번째 회의를 진행하였으며, 중국 전문가가 컨비너와 간사를 맡고 있다. 총 16개국에서 81명이 참여하고 있으며, 한국에서는 7명이 1차회의 때 참가한 것으로 되어있다. 1차 회의 때 6개의 Recommendation이 승인되었으며, 10개의 liaison 이슈가 있었다. 10개의 liaison에 진행되고 있는 양자기술관련 활동을 위해 3개월마다 회의를 개최하며, 2020년 12월에는 3차 WG14 회의를 진행하였다. 현재 용어와 어휘에 대한 표준 (ISO/IEC WD 4879, Quantum computing - Terminology and vocabulary)하나 만을 개발 중에 있으나, 향후에는 quantum architecture, quantum internet, quantum algorithm, QC use cases 등 표준을 개발할 예정이다. 10 Liaison issues은 JTC1/SC7, JTC1/SC27, ITU-T SG17, ITU-T SG13, ITU-R FG-QIT4N, IEEE P1913, IEEE P7130, IEEE P7131, ETSI ISG, TC Cyber WG QSC, CEN CENELEC/FGQT 등이다[2][4].

ISO/IEC의 JTC 1/SC 27(정보보안기술)에서는 양자키분배 보안 요구사항, 시험 및 평가방법 등 2개의 표준이 개발되었다. SC27 (Security techniques)에서는 양자키분배 보안 요구 사항, 시험, 평가 방법에 대한 학습기간 운영 중(`18.4 총회)이며, 양자암호 통신의 실용화 이슈가 논의되었다. SC7 (Software systems and systems engineering)에서는 SG(Study Group)을 구성하여 SC7의 활동 범위에 부합하는 표준화 활동 모색 중이다[2][4].

IEEE에서는 P1913(소프트웨어로 정의된 양자통신), P7130(양자컴퓨터 용어정의), P7131(양자컴퓨터 성능측정방법) 등에서 양자통신과 양자통신의 표준화 이슈를 함께 논의하고 있다[7].

ETSI (유럽전기통신표준협회)에서는 장비제조사 및 학계 중심으로 양자암호 시스템 표준화를 진행하고 있으며[14], ISG (Industry Specification Group) 양자키분배 기술 관련 20개의 규격을 제정하였다[5]. GS QKD 003 (부품), 007 (용어), 010 (장비해킹), 012 (장비운용), 013 (송신기규격), 014 (암호전달 프로토콜) 등이 진행되고 있다. QKD 중심의 논의 진행 중이며, Toshiba, NTT를 비롯한 유럽과 중국, 캐나다 기업과 연구소 등이 참여하고 있다[5]. 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[13].

표 2. ETSI 표준 발행[5]

번호	표준명	발행일
GS QKD 012	Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment	`19.2
GS QKD 014	Protocol and data format of REST-based key delivery API	`19.2
GR QKD 007	Vocabulary	`18.12
GR QKD 003	Components and Internal Interfaces	`18.3
GS QKD 011	Component characterization : characterizing optical components for QKD systems	`16.5
GS QKD 008	QKD Module Security Specification	`10.12
GR 006	Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes	'17.2
GS QKD 005	Quantum Key Distribution (QKD); Security Proofs	`10.12
GS QKD 004	Application Interface An update is in preparation	'20.8
GR 004	Quantum-Safe Cryptography; Quantum-Safe threat assessment	`17.3
GS QKD 002	Quantum Key Distribution (QKD); Use Case	`10.6
GR 001	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework	'16.7
TR 103 617	Quantum-Safe Virtual Private Networks	'18.9
TS 103 744	CYBER; Quantum-safe Hybrid Key Exchanges	'20.12
GR QSC 003	Quantum Safe Cryptography; Case Studies and Deployment Scenarios	'17.2

번호	표준명	발행일
TR 103 619	CYBER; Migration strategies and recommendations to Quantum Safe schemes	'20.7
EG 203 310	CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection	'16.6
TR 103 570	CYBER; Quantum-Safe Key Exchanges	'17.10
TR 103 618	CYBER; Quantum-Safe Identity-Based Encryption	'19.12
TS 103 485	CYBER; Mechanisms for privacy assurance and verification	'20.8

Ⅲ. 결 론

양자기술관련 국제표준화 동향에 대하여 알아보았다. 이를 통해 IEC, ISO, ITU-T, ETSI, IEEE 등에서 활발하게 양자컴퓨팅과 양자통신과 관련된 국제표준화 활동이 진행되고 있는 것을 알 수 있었다. 특히, ISO/IEC JTC1 WG14 (양자컴퓨팅) 에서 2020년에 양자컴퓨팅 관련 표준화를 시작하여 현재 용어 정의와 어휘에 대한 표준화 (ISO/IEC WD 4879, Quantum computing - Terminology and vocabulary))를 추진하고 있다. 향후에는 quantum architecture, quantum Internet, quantum algorithm, QC use cases 등에 표준을 개발할 예정이다. 또한, JTC1/SC7, JTC1/SC27, ITU-T SG17, ITU-T SG13, ITU-R FG-QIT4N, IEEE P1913, IEEE P7130, IEEE P7131, ETSI ISG, TC Cyber WG QSC, CEN CENELEC/FGQT 등과의 Liaison ship을 추진할 예정이다. 이들 중에서 한국은 ITU-T와 ETSI 등에서 국제표준화 활동을 활발하게 참여하고 있다.

양자기술에서는 양자통신, 양자컴퓨팅, 양자센싱 등 다양한 분야를 다루기 때문에 기존에 존재하는 기술위원회 (Technical Committee)와 중복이 되지 않거나 최소화하는 방향에서 우리나라가 ISO/IEC JTC1이나 IEC 등의 공적표준화 기구 안에서 양자기술 (Quantum Technology) 관련 기술위원회 (Technical Committee) 제안과 설립을 추진한다면, 양자기술 분야 국제표준화에 있어서 주도적인 역할을 할 수 있을 것 사료된다.

Acknowledgements

본 원고와 관련하여 산업통상자원부, 국가기술표준원, 그리고, 한국표준협회에서 주관하는 2020년 국가표준기술력향상사업을 통해 연구비 지원을 받았습니다. 연구비 지원에 감사드립니다. 또한, 원고 작성에 많은 도움을 주신 한국전자통신연구원의 박성수 단장님께도 감사드립니다.

참 고 문 헌

[1] 한국표준협회 홈페이지, www.ksa.or.kr/ksa_kr/942/subview.do
[2] IEC 홈페이지, www.iec.ch
[3] 국가기술표준원 홈페이지, www.kats.go.kr
[4] ISO 홈페이지, www.iso.org
[5] ETSI 홈페이지, www.etsi.org
[6] ITU-T 홈페이지, www.itu.int
[7] IEEE 홈페이지, www.ieee.org
[8] NIST 홈페이지, www.nist.gov
[9] CSA 홈페이지, www.csagroup.org
[10] 윤빈영, "ITU-T SG15 양자키 분배 표준화동향", ICT Standard Weekly (TTA) 제910호. pp. 1 ~ 2
[11] 심동희, "ITU-T SG17 양자 암호 표준화 동향", 정보보호학회지, 제 29 권 제4호, 2019. 8, pp. 25 ~ 28
[12] 한국정보통신기술협회 홈페이지, www.tta.or.kr
[13] 김민형, "양자암호통신 테스트베드 및 표준화 동향", AI Network Lab 인사이트 제5호 (NIA) (2019.07), pp. 1~22.
[14] IITP주관 양자정보통신 기술로드맵 위원회, "ICT R&D 기술로드맵 2025", (2020), p.132~176.

약 력

박 준 식

공동교신저자
1992년 한양대학교 재료공학 공학사
1994년 한양대학교 재료공학 공학석사
2004년 한양대학교 재료공학 공학박사
1994년~현재 한국전자기술연구원 스마트센터연구센터 수석연구원
2007년~2009년 스탠포드대학교 재료공학과 Visiting Scholar
관심분야: 마이크로/나노 환경센서, 양자센서

황 태 호

공동교신저자
1998년 한국외국어대학교 컴퓨터공학과 학사
2000년 한국외국어대학교 컴퓨터공학과 석사
2013년 한국외국어대학교 컴퓨터공학과 박사
2000년~2018년 한국전자기술연구원 SoC플랫폼연구센터 수석연구원
2018년~현재 한국전자기술연구원 SoC플랫폼연구센터 센터장
관심분야: 실시간 운영체제, 이기종 컴퓨팅, 뉴로모픽 컴퓨팅

주 정 진

1990년 부산대학 물리학 학사
1992년 부산대학 물리학 석사
1997년 부산대학교 물리학 박사
1997년~1998년 한국표준과학연구원 Post-Doc.
1999년~2000년 7월 포항공과대학 연구원
2000년~현재 한국전자통신연구원 선임/책임/실장
관심분야: 양자광학 및 광집적회로 소자

이 택 민

1995년 한국과학기술원 정밀공학 공학사
1997년 한국과학기술원 기계공학 공학석사
2002년 한국과학기술원 기계공학 공학박사
2002년~2003년 MIT 기계공학과 Post Dr.
2003년~현재 한국기계연구원 책임연구원
관심분야: 인쇄전자, 양자센서

한 지 수

2016년 상명대학교 컴퓨터공학 공학사
2016년~현재 한국전자기술연구원 연구원
관심분야: 뉴로모픽 컴퓨팅, 실시간 운영체제, 양자센서