ETRI

2019
Electronics and
Telecommunications
Trends

양자정보통신기술 현황과 전망

Status and Prospects of Quantum Information Communication Technologies(Q-ICT)

박성수 (S.S. Park, sspark@etri.re.kr) 미래기술연구본부 책임연구원
송호영 (H.Y. Song, hsong@etri.re.kr) 미래기술연구본부 책임연구원/본부장

Ⅰ. 서론
Ⅱ. 정책 동향
Ⅲ. 양자통신 기술 동향
Ⅳ. 양자컴퓨팅 기술 동향
Ⅴ. 양자센서 기술 동향
Ⅵ. 결론

Commercial services providing quantum cryptographic communication are available in China and the United States of America (USA), and a commercial cloud service for quantum computing is available in the USA. This has been possible since the early stage prototypes of quantum technologies have transitioned from theory to practical applications. This has led to the development of a new industrial ecosystem so that governments are announcing plans to support further research and development, new ventures are being launched, and a market is emerging. We will discuss the technological possibilities of future developments from the early-stage achievements.

* DOI: 10.22648/ETRI.2019.J.340207

본 저작물은 공공누리 제4유형
출처표시+상업적이용금지+변경금지 조건에 따라 이용할 수 있습니다.

©2019 한국전자통신연구원

Ⅰ. 서론

2018년 10월 미국 Quantum Xchange사는 뉴욕시의 월가와 뉴저지의 백오피스 간 양자암호를 적용한 금융거래 및 영업정보에 대한 비밀통신서비스를 시작하였다[1]. 한편, 미국 IBM은 2016년 5큐빗의 양자컴퓨터를 일반에 공개한 데에 이어, 2018년 5월 양자컴퓨터의 상업적 사용을 지원하기 위한 5개 지역 허브와 본사 등 총 6개 센터를 만들고, 삼성, 어센추어, 엑슨모빌, JP모건 등 굵직한 기업들이 유료 사용자로 되어 있다[2]. 또한, 2019년 1월에는 상업용 양자컴퓨터 시제품인 IBM Q System One을 공개하였다[3]. 이러한 상용제품들이 출시되기까지 2000년 초반부터 시작된 수 많은 연구개발의 노력이 결실을 맺었기에 가능하다. 그동안 어떠한 기술적 진전이 있었는가와 향후의 발전 가능성에 대해서 생각해 본다.

'양자정보통신'은 양자의 물리학적 성질(중첩, 얽힘, 복제불가 등)을 직접적으로 정보처리와 통신에 이용하는 기술을 일컫는 것으로 우리나라에서만 부르는 용어이다. IT 기술을 정보통신기술로 부르는 것과 같은 용어사용 방법이라고 볼 수 있다. 〈표 1〉에서는 각국의 정책보고서에서 말하고 있는 양자정보통신에 대한 용어 및 의미에 대해 정리해 놓았다. 미국은 양자정보과학(Quantum Information Science), 유럽은 양자기술(Quantum Technology) 등 국가별로 양자정보통신을 지칭하는 용어가 다르나, 공통적으로 양자통신, 양자컴퓨팅(시뮬레이터 포함), 양자센서 등을 포함하고 있다. 2018년 5월부터 IITP에서는 양자정보통신 로드맵을 국내 전문가들과 협의하에 작성하여 12월에 발표하였다[4]. 이에 따르면 양자통신에는 양자암호, 양자전송, 양자네트워크 등 3개 세분류, 양자센서/이미징에는 양자측정, 양자센싱, 양자이미징의 3개 세분류, 양자컴퓨팅은 양자시뮬레이션, 물리양자비트, 논리양자비트, 양자소프트웨어 등의 4개 세분류로 되어 있다.

Ⅱ. 정책 동향

초기 시제품의 성과와 이를 바탕으로 향후에는 기존 IT 기술을 넘어설 수 있다는 신기술로서의 잠재적 가능성을 높이 평가하여 각국은 여러 가지 정책을 발표하였다.

미국은 2008년 12월 국가과학기술위원회에서 '양자정보과학의 연방비전'[5]을 발표하여 기술의 잠재력을 이끌어내고 신기술에 대한 미국의 리더십 보장을 당부한 이래, 2016년 7월 오바마 정부의 백악관은 양자정보과학의 추진과 정책적 지원을 발표[6]하고, 트럼프 행정부에서도 양자정보과학의 국가전략을 발표하여 각 정부부처의 지원정책 간 조율, 교육, 연구개발센터 등 정책지원을 위한 기본계획이 되도록 하였다[7]. 특히, 2018년 12월 트럼프 대통령이 서명한 양자이니셔티브법[8]이 통과되어 5년간 약 12억달러 예산을 가진 종합적이고 일관된 정책을 갖게 되었다.

유럽은 그동안 국가별로 따로 지원하고 있었으나 전 유럽이 공동으로 개발할 수 있는 10억유로 규모의 H2020 플래그십 과제로 발전시켜 2018년 10월부터 2021년 9월까지 3년간 1단계 사업[9]이 시작되었다. 영국은 2014년부터 2018년까지 지원한 4개의 양자허브 대학을 2024년까지 5년 더 지원하기로 하였고, 이와는 별도로 국립양자컴퓨팅센터, 박사급 교육센터, 산업화지원 등으로 약 3억2천만파운드의 지원정책을 2018년 11월에 발표[10]하였다.

중국은 안후이省 허페이市에 2020년까지 약 10만 평 규모의 양자정보국가연구소를 건설하고 잠

〈표 1〉 국가별 양자정보통신 관련 기술 정의

국가	양자 지칭 기술 용어	정의	세부내용	관련 정책보고서
미국	양자정보과학 (QIS: Quantum Information Science)	양자역학과 정보이론이 합쳐진 기술	• 센싱 및 계측 • 통신 • 시뮬레이션 • 컴퓨팅	양자정보과학의 추진: 국가적 도전과 기회('16.07)
EU	양자기술 (Quantum Technology)	양자역학의 성질을 실제 응용분야에 사용 가능하도록 변환시키는 새로운 기술	• 통신 • 컴퓨팅 • 시뮬레이션 • 센싱 및 계측 • 기초과학	양자기술 플래그십 최종보고서 ('17.06)
영국	양자기술 (Quantum Technology)	양자2.0*을 이용하는 기술	• 양자시계 • 통신 • 센서 • 컴퓨팅, 시뮬레이션, 정보처리	영국 양자기술 현황 2014('14.02)
독일	양자기술 (Quantum Technology)	개별 양자계에 영향을 미칠 수 있는 (새로운) 양자기술**	• 통신 및 암호 • 정보 및 컴퓨터 • 고체 내 양자정보처리 • 이론 및 수학원리 • 양자제어 • 원자양자센서 및 물질파 광학 • 특수양자기술	양자기술: 연구에서 응용까지 ('15.06)
일본	양자과학기술 (量子科学技術)	"양자"의 행동이나 영향에 관한 과학 및 그것을 응용하는 기술 (「量子科学技術」とは、「量子」のふるまいや影響に関する科学とそれを応用する技術である。)	• 양자정보처리 · 통신(양자컴퓨팅, 양자시뮬레이션, 양자통신 · 암호) • 양자계측 · 센싱 · 이미징(생물 · 생명과학계, 물리계) • 최첨단 포토닉스 · 레이저(광원의 첨예화 및 새로운 광기능의 발현 · 제어, 산업 응용의 고도화)	양자과학기술(광 · 양자기술)의 새로운 추진방안 ('17.08)
중국	양자제어 및 양자정보 (量子调控 与量子信息)	양자현상을 직접 제어할 수 있는 기초기술과 이를 통신, 정보, 센싱에 응용하기 위한 양자정보기술을 통틀어서 양자제어 및 양자정보로 부름	• 관련 전자시스템 • 소규모 양자시스템 • 인공 밴드갭 시스템 • 양자통신 • 양자컴퓨팅 및 시뮬레이션 • 양자정밀측정	13차 5개년 국가과기 혁신규획 (2016-2020)

* 양자1.0: 양자역학 기본원리로부터 핵물리, 원자, 분자, 고체물리, 빛과 물질 상호작용 등을 연구하는 양자물리

양자2.0: 양자중첩, 양자얽힘, 양자제노효과, 진공은 빈 공간이 아님 등의 성질을 연구하는 양자물리

** 1세대 양자기술은 양자물리에 기반하여 반도체, 레이저의 기반기술이었으나, "새로운" 양자기술은 개별 양자시스템에 대해 (직접) 영향을 미칠 수 있는 기술로 향후 20년간 발전해 나갈 것

수함용 양자네비게이션, 암호해독용 양자컴퓨터 등을 개발할 예정[11]이다.

일본은 광 · 양자 비약 플래그십 프로그램(Q-LEAP)을 발표[12]하고 2018년부터 10년간 약 220억엔을 투자하여 양자컴퓨터와 양자센서를 개발할 예정이며, 위성통신통신에서의 양자암호 기술의 연구개발과제로 2018년부터 5년간 약 16억엔을 들여 양자위성체와 관제기술을 개발할 예정[13]이다.

2018년 12월 이스라엘 정부도 군사적 우위 확보를 위해 5년간 1억이스라엘셰켈을 투자하여 대학의 연구장비 업그레이드와 국방부 선정과제에 대한 연구개발 투자를 발표[14]하였다.

〈표 2〉 각 국의 최신 정책추진 내용

국가	이전 추진 내용	향후 추진 내용	예산	기간
미국 [5]–[8]	• IARPA, NIST, NSF의 산발적 연구지원 • 대학별 각자 연구 수행	• NIST(학연협력연구), DOE(양자연구센터), NSF(인력양성) 역할구분 • 백악관 중심의 조정기구설치	12억달러 (1.35조원)	’19–’23
중국 [11]	• 양자컴퓨터는 각 대학별 기초기술 집중 • 양자통신은 상해–북경 간 중국산 장비 개발 후 적용(중국과학원, 중국과기대 중심)	• 중국과학원 중심의 양자전문연구소 설립 • 시진핑의 적극 지원	76억위안 (1.26조원) 연구소설립만	’17–’20 연구소설립만
영국 [10]	• 4개의 허브 대학 중심 연구	• 4개 허브는 유지하되 연구규모 축소 • 양자컴퓨팅센터 설립 • 박사급 교육 지원 • 산업화 지원	2.35억 파운드 (3,400억원)	’19–’24
유럽 [9]	• 각국별로 소규모 연구	• H2020의 플래그십 과제화(3개 중 1개) • 1단계는 대학 위주로 진행되나 2, 3단계부터는 기업 참여 확대	10억유로 (1.28조원)	‘18–’27
일본 [12], [13]	• ImPACT 등 대규모 사업 중 일부로 수행 • 대학 위주 연구	• 정부주도로 플래그십과 기초연구 과제를 포함한 단독 사업(Q-LEAP) 추진 • 양자위성통신 추진	235억엔 (2천4백억원)	’18–’27
이스라엘 [14]	• 활동 없음	• 대학의 연구그룹 참여 확대 • 양자를 군사력 증강의 전략적 목표화	1억세켈 (306억원)	’19–’23
대만	• 활동 없음	• TSMC와 IBM의 공동연구 추진 • 3개 국립대학 연구	0.6억 타이완달러 (22억원)	’19–’23
인도 [15]	• 활동 없음	• 1단계 4개 과제 3년 연구 지원 후 2단계에 본격지원	80크로네 (128억원) 300크로네 (513억원)	’19–’21 (1단계) ’22–’28 (2단계)

인도는 2019년 1월부터 80크로네를 들여 3년간 기반기술 확보와 인력 부족을 해소하고, 그 후 총 300크로네 규모의 기술개발을 통해 세계적 수준으로 도약을 준비하였다[15]. 〈표 2〉에 각국의 최신 정책추진 내용을 정리하였다.

Ⅲ. 양자통신 기술 동향

1. 양자통신 기술 현황

양자통신기술은 양자암호통신기술과 양자전송 및 네트워크 기술로 나눌 수 있다. 양자암호통신기술은 양자의 성질 중 복제불가를 이용한 BB84 프로토콜 기술과 얽힘 광자를 이용한 E91 등 여러 가지 기술이 제안되고 있다. 그중 BB84 프로토콜과 다양한 변종이 양자암호통신을 위한 상용제품으로까지 발전하였다. 양자전송 및 네트워크에서는 얽힘의 상관관계를 이용하여 양자상태를 전송할 수 있고 여러 경로를 연결할 수 있는 기술로서 아직 기초기술연구에 머물러 있다.

양자암호통신은 이론적으로는 무조건적 안전성을 보장한다고 하지만, 암호화할 데이터의 전송속도보다 키생성속도가 매우 느려서 OTP(One Time

Password)로써 역할을 할 수 없고, 부채널 공격에도 여전히 취약하며, 현재의 공개키인프라(PKI: Public Key Infrastructure)와 VPN(Virtual Private Network)에 의한 활용도보다 떨어지므로 널리 사용될 수 없다는 논의[16]가 있었다.

암호통신의 단계는 계산복잡성에 의한 보안, 정보이론적 보안, 무조건적 안전의 3가지 단계가 있다. 즉, 무조건적 안전성을 보장하려면 무한한 계산능력을 가진 정보 탈취자로부터 안전해야 하는데, 계산의 어려움이나 복잡성에 의존하는 PKI나 VPN은 정보보호에 취약할 수밖에 없다. 다음 단계인 정보이론적 보안은 광CDMA전송과 같은 물리계층에서의 보안을 말하는데, 이 경우 현재 기술로는 어렵겠지만 수 dB의 SNR(Signal to Noise Ratio)를 개선할 경우 충분히 암호를 해독할 수 있다는 연구결과[17]를 볼 때 안전하지 않다는 것을 알 수 있다. 마지막 단계인 BB84 양자암호분배 기술과 디바이스 독립 양자암호분배 기술을 사용한 경우가 무조건적 안전한 기술이 될 수 있다. 한편, 부채널 공격에 대해서는 어떠한 보안장비라고 하더라도 구현에 따른 결함을 가지고 있으므로 안전할 수는 없다. 따라서, 양자암호통신장비가 부채널 공격에 취약하기 때문에 양자암호를 쓸 수 없다는 것은 논리의 비약일 수 있다. 물론, 양자암호분배에 대한 부채널 공격인 트로이목마[18], [19], 수신기효율부조화[20]-[23], 위상재매핑[22], [24], [25], 블라인딩공격[22], [26] 등이 있으나 이에 대해서도 많은 연구를 통해 보완하고 있다. 또한, 키생성속도가 낮은 것은 적절한 현대암호의 키증폭 방법에 의해서 가능하다고 알려져 있어서 양자암호분배가 가장 보안성이 높은 통신방법으로 볼 수 있다.

또한, 전송거리 측면에서 리피터를 사용하지 않고 보낼 수 있는 최대 거리를 550km까지도 확장 가능한 TF(twin field)-QKD 프로토콜을 발표[27], [28]하기도 하여 그동안 실험으로 발표된 도시바의 421km, 제네바 대학의 307km보다 더 멀리 보낼 수 있다. 그러나, 기존의 BB84 기반이 아니므로 무조건적으로 안전하다는 것에 대한 증명이 남아 있다.

2. 양자통신 테스트베드

유선광통신망에 의한 양자암호통신은 2000년대 초반부터 미국과 유럽을 중심으로 일찍이 기술개발이 시작되었다. 이들 개발된 기술은 실제 사용환경에서의 시험검증이 필요하다. 이러한 테스트베드는 기술개발의 순기에 따라 실험망(기술개발 및 시연) → 시험망(장거리 시연 및 네트워크 안정성 시험) → 시범망(응용 서비스 실증) → 상용망(상용서비스 제공)으로 구분할 수 있다. 〈표 3〉에서는 개발단계별 각국의 유선, 무선 QKD 및 양자전송의 테스트베드 구축현황을 정리하였다.

3. 양자통신 표준화 현황

양자암호통신에 대해 유럽의 ETSI(European Telecommunications Standards Institute)에서 2010년경에 ISG(Industry Specification Group) 수준의 규격 표준화를 시작하였고, 2018년부터 국가 간 표준화 기관에서 양자암호통신에 대한 표준 논의가 진행되기 시작하였다. 다음 목록에 표준화 기관과 표준화 그룹에 대해 정리하였다. 특히, 중국은 상해-북경 간 2,000km 양자백본을 자체 개발한 양자암호통신 장비로 구축하였고, 그 여세를 몰아 자국의 기술을 국제표준화하려고 적극 나서고 있다.

〈표 3〉 각국의 양자통신 관련 테스트베드 현황

분야	국가	실험망	시험망	시범서비스 실증망	상용서비스망
유선 양자 암호 (QKD)	미국	• DARPA 시연 ('02–'07)	• 콜럼버스시 네트워크 시험 ('13) • 콜럼버스–워싱턴DC 장거리 ('15)	• 퀀텀익스체인지특허정보 관련 시범서비스('18)	• 퀀텀익스체인지월가 서비스 ('18–)
	유럽	• SECOQC 시연 ('04–'08) • 스위스선거시연 ('07)	• 스위스퀀텀 안정성 시험 ('09–'11) • 이탈리아 장거리 시험망 ('13–'16)	• AVDA 2,800km전송서비스 ('18)	–
			• Quantum Internet Alliance ('18–'20)		
	일본	• Tokyo QKD Network('10–) 개방형 실험/시험망		• NEC데이터센터 서비스('15) • 도시바–동북대 의료데이터 서비스('15) • H–LINCOS ('18)	–
	영국	• 아다시트랄–입스위치 시연 ('14)	• 브리스톨–캠브리지 장거리 시험('13–'18)	• 아다스트랄–캠브리지 은행서비스 ('17)	–
	중국	• 중국과기대 시연('09)	• 중국과기대 5개 노드 네트워크('10) • 허페이('12), 진안('13) 네트워크 시험	• 상해–북경 간 QBN('12–'17)으로 은행망, 통신사의 양자암호통신 서비스('18–)	
유선 양자 전송	미국	• FQNET ('18–'20)	• INQNET ('17–'23)		
	이탈리아	• 말타–시실리 96km ('18)	• QIA ('18–'20)		
	캐나다	• 캘거리대 17km ('16)			
무선 양자 전송	중국	• Micius 1200km ('17)			
	싱가폴	• 싱가폴국립대 ('09)			
	유럽	• 144km 카나리제도 무선전송 ('07)			
위성 양자 전송	중국	• 631kg Micius ('17)			
	일본	• 48kg SOCRATES ('17)	• 이동형 양자위성탑재체 ('18–'22)		
	오스트리아	• 4kg Q3Sat 큐브샛 ('18)			

- ETSI GS QKD 003(부품), 007(용어), 010(장비해킹), 012(장비운용), 013(송신기규격), 014(암호전달프로토콜)
- TTA TC2(통신망), PG201(광전송), TC5(정보보호), PG501(정보보호기반)
- ITU–T SG13(미래인터넷), SG15(전달, 액세

스), SG17(보안)

- ISO/IEC JTC1 SC27(정보보안, CC인증도 같이 함)
- IEEE P1913(소프트웨어로 정의된 양자통신), P7130(양자컴퓨터 용어정의), P7131(양자컴퓨터 성능측정방법)
- CSA(클라우드보안연맹), QSSWG(양자내성보안 워킹그룹)

특히, IEEE는 양자암호통신뿐만 아니라 양자컴퓨터에 대해서도 용어 정의나 성능측정방법에 대한 표준화도 추진하고 있다.

4. 양자통신 전망

중국과 미국에서 상용망 서비스가 전개됨에 따라 BB84 프로토콜 및 그 변종에 의한 양자암호통신은 표준화까지 더하게 되어 기술완성도를 더욱 높일 수 있게 되었다. 그러나 양자기기(센서 및 컴퓨터 등) 간의 양자상태를 주고받을 수 있는 양자네트워크, 양자얽힘을 사용한 더욱더 안전한 양자암호 등의 기술에 대해서는 아직도 기술 개발해야 할 부분이 많이 남아 있어서 장비로까지 개발되기에는 시일이 오래 걸릴 것이다. [29]에는 일본 NICT에서 밝힌 양자네트워크의 발전전망을 보여주고 있고, 일반적으로 양자통신의 로드맵은 1:1 암호통신 → 신뢰노드를 통한 1:1 장거리 암호통신 → 가입자망 및 무선가입자를 포함한 암호통신 → 양자기기(센서, 컴퓨터 등) 간 단거리 네트워크 → 양자라우터에 의한 장거리 네트워크 → 양자인터넷으로 변화할 것으로 전망된다. 미국과 중국의 양자암호통신서비스는 2번째 단계까지 도달한 상태이다.

Ⅳ. 양자컴퓨팅 기술 동향

1. 양자컴퓨팅 기술 현황

양자컴퓨터 분야에서는 1990년대의 이론적 가능성 연구, 2000년대의 POC(Proof of concept) 연구, 2010년대의 안정화 및 확장성 연구를 통해 실제로 작동하는 양자컴퓨터 초기 시제품을 만들어내게 되었다. 양자의 특수한 성질을 이용하기만 하면 양자컴퓨팅으로 볼 수 있기 때문에 다양한 방식의 양자컴퓨터가 존재하고 있고, 이를 지칭하는 용어가 혼용되어서 사용되기도 한다. 따라서, 〈표 4〉에 종류 및 개략적인 현황을 정리하였다. 양자어닐러와 같은 개념을 디지털 회로로 흉내 낸 디지털어닐러가 2018년 발표되었는데, 양자어닐러보다 장점이 있고 응용 가능성이 있어서 분류에 포함시켰다.

각 연구 기관별 양자컴퓨터의 개발 현황[30]을 살펴보면, 초전도 큐빗에서는 IBM, 인텔, 구글이 50여 큐빗, Rigetti, 중국과기대가 10여 큐빗을 개발하고, 이온트랩은 IonQ, 옥스포드 대학, 인스브룩 대학 등에서 20여 큐빗을 개발하였고, 그밖에 중성원자에서는 하버드 대학, 위스콘신 대학 등에서 50여 개 큐빗을 개발하였다. 한편 SW시뮬레이션에서는 알리바바, Atos, ETH, IBM, 인텔, Microsoft, 멜버른 대학, Rigetti 등에서 40~150큐빗을 에뮬레이션할 수 있도록 개발되었고, 대부분 100큐빗급까지 개발될 것으로 보인다.

2. 양자컴퓨팅 클라우드 서비스 현황

IBM, Rigetti, D-Wave, IonQ 등은 자사의 양자컴퓨터 초기 시제품 HW 및 관련 SW를 개방하여 인터넷으로 활용할 수 있는 클라우드 서비스를 제공하여 양자컴퓨터의 사용자 확보 및 큐빗 품

〈표 4〉 양자컴퓨터의 종류 및 현황

종류	설명	주 사용 분야	작동환경	주요기관
Gate 방식 양자컴퓨터	큐빗에 대해 양자 로직 게이트 연산 적용을 통해 양자상태를 변경시킴으로써 양자계산을 수행하는 것으로 고전컴퓨터의 논리 게이트 적용으로 계산이 수행되는 것과 유사. 양자게이트는 X, Y, Z, S, T, H, CNOT 등이 있음. 연산방법은 회로모델, 1방향연산모델 등이 있고, 에러율 저하와 양자상태 유지시간 향상 연구 등이 중요	소인수분해 데이터 검색 행렬계산 추천알고리즘 양자게임 암호해독(예상) 인공지능(예상) 빅데이터(예상)	극저온 차폐환경 또는 저온/진공 저압환경	IBM 구글 Regetti IonQ Oxford 인스브룩대 인텔 MS
양자 시뮬레이터	다체(many body)문제 등 양자화학, 양자물리의 문제를 풀기 위해 큐빗으로 모델링하고 양자 연산을 통해 양자적 거동을 직접 수행함으로써 문제를 푸는 양자시스템	촉매 거동 해석 광합성 해석 원자핵 분석		하버드 IonQ
양자 어닐러	풀고자하는 문제를 큐빗에 의한 에너지의 분포로 표현하고 에너지 최소 상태를 양자 터널링 등의 방법으로 순식간에 찾아냄으로써 계산을 수행되는 컴퓨터. 여러 가지로 차선의 해법이 있어서 최선의 최적화 해법을 찾기 어려운 문제에 적용 시 효과를 발휘	물류 최적화 공정 최적화 투자포트폴리오	극저온 차폐환경	D-Wave 구글
디지털 어닐러	양자 어닐러와 같은 방법으로 표현된 에너지 분포에 대해 몬테카를로법 등 다른 방법으로 에너지 최소 상태를 찾아내는 방법. 양자적 방법은 아니지만 상온동작, 스케일업, 디지털컴퓨터와의 통합 등에서 유리한 점이 있음	상동	상온 고전컴퓨터 작동 환경	후지쯔
SW 시뮬레이터	게이트 방식 양자컴퓨터의 기능(큐빗의 중첩, 얽힘 등)을 PC, 클라우드, 슈퍼컴퓨터 등의 고전컴퓨터에 SW적으로 구현한 시뮬레이터. 50큐빗 정도 얽힘을 표현하더라도 140테라바이트의 메모리가 필요하므로 무한정 많은 큐빗을 표현할 수 없음	게이트 방식 양자컴퓨터와 동일	상온 고전컴퓨터 작동 환경	MS IBM Atos 알리바바

질 향상을 위한 피드백을 받고 있다. 이 중 IBM은 상업 서비스인 IBM Q Experience를 시작하였다. 2016년 5월 5큐빗 초전도 양자컴퓨터 클라우드 서비스를 일반에게 공개하였고, 2018년 5월부터 12, 16, 20큐빗 초전도 양자컴퓨터를 5개의 지역허브(뮌헨 대학, 노스캐롤라인주립 대학, 오크리지국립연구소, 멜버른 대학, 옥스퍼드 대학, 게이오 대학)와 본사 등 총 6개의 센터에서 유료 회원사에 양자컴퓨터 사용권 제공 및 기술지원 중이다[2]. Rigetti는 2017년 19큐빗 초전도 양자컴퓨터를 공개하였으나 서비스를 중단하고 2018년 6월 8큐빗 초전도 양자컴퓨터를 공개한데 이어 2019년 1월에는 SW 툴을 공개하고 30여 명의 베타 사용자에게 1개월간 5,000달러 상당의 사용권을 제공하고 있다[31]. 또한, Rigetti는 초전도 큐빗의 성능을 대폭 향상시켜 T1을 100μs, 2큐빗 연산 피델리티 99.2%를 발표[32]하였다. D-Wave는 2018년 10월 2,000큐빗 초전도 양자어닐러 클라우드 서비스를 개발자에게는 무료로, 상업적 이용에 대해서는 월간 1시간에 대해 2,000달러로 제공하는 서비스를 발표[33]하였다. IonQ는 2019년 초에 11개 이온큐빗(2큐빗 피델리티 98%) 양자클라우드 서비스를 선정된 베타 사용자에게 제공[34]하기 위해 지원자 모집 중이다. 또한, 2018년 2월부터 중국과학원의 11큐빗 초전도 양자프로세서와 알리바바의 SW 툴과 클라우드 서비스 기술로 서비스[35]하고

있다. 한편, 영국의 브리스톨 대학에서는 6큐빗의 광양자컴퓨터에 대해 실제 동작하는 광양자컴퓨터 뿐만 아니라 SW 시뮬레이션 서비스를 'Quantum in the Cloud'라는 이름으로 제공하고 있다[36]. 특기할 만한 사실은 잡음환경을 고려한 계산결과를 SW 시뮬레이션해 볼 수 있는데, 다음에 설명할 NISQ(Noisy Intermediate-Scale Quantum) 양자컴퓨터의 성능을 가늠해 볼 수 있을 것이다.

3. NISQ(Noisy Intermediate-Scale Quantum) 시대

2018년 1월 칼텍의 John Preskill 교수는 현재 개발된 양자컴퓨터의 성과를 높이 평가하고 활용성을 찾아주기 바라는 뜻으로 NISQ 시대라고 명명[37]하였다. 이것은 에러가 정정되지 않은 50~100큐빗의 중간규모 양자컴퓨터 시대라는 뜻으로 양자컴퓨터의 잠재력에 대해 설명하고, 결함허용 양자컴퓨터까지는 아직 먼 꿈이지만 이제 중요한 방점을 찍은 상태로서 슈퍼컴퓨터로 구현 가능한 수준인 50큐빗을 넘어서게 되었다는 것과 에러율이 0.1%라고 하더라도 1,000큐빗이라면 적어도 1개 큐빗은 에러라는 뜻이 되므로 계산결과를 신뢰할 수 없게 되는데(현재 에러율은 그보다도 훨씬 높아서 수 %에 이른다), 이러한 잡음 환경을 고려해야 하는 것 등을 지적하였고, 이외에도 NISQ 양자컴퓨터에 의한 계산속도향상을 가져올 수 있는 수학계산 분야는 최적화, 양자어닐링, 잡음탄력양자회로(Noise-Resilient Quantum Circuit), 양자딥러닝, 양자역행렬, 양자추천, 양자 Semidefinite 프로그래밍, 양자시뮬레이션, 양자게임 등에서 가능할 것으로 말하고 있다. 이러한 사실로 미루어 볼 때, 양자컴퓨터는 모든 계산을 만능으로 할 수 있는 것이 아니고 제한된 수학계산에서 위력을 발휘할 수 있다는 것이다.

특이한 것으로, 2018년 7월, 18세의 Ewin Tang[38]은 양자추천 알고리즘이 양자적 알고리즘임에도 불구하고 고전컴퓨터에서도 구현 가능하고 지수함수적으로도 빠르다는 것을 밝혀서 양자에 기반한(quantum-inspired) 고전알고리즘으로도 구현 가능한 알고리즘들에 대한 추가 연구가 진행 중이다.

4. 양자컴퓨터 전망

2018년 12월, 워싱턴 정가를 위한 국가자문, 의견수렴 등을 지원하는 비영리 단체인 과학, 공학, 의약 아카데미는 미국국가정보국의 지원을 받아 구글의 John Martinis 교수, MS의 Krysta Svore 등 약 50여 명 전문가의 의견을 참고하여 'Quantum Computing: Progress and Prospects'라는 보고서를 발간[39]하였다. 양자컴퓨터의 전산 모델링은 1980년대에 제안되었고, 1990년 Shor알고리즘으로 암호해독 가능성을 제시한 이래 25년이 지난 지금, 시연 가능한 큐빗을 만들 수 있게 되었으며, 민간에서도 많은 투자를 하게 되었다. 그러나, 향후 발전전망을 위해서는 해결해야 할 문제를 다음과 같이 제시하고 있다. 2큐빗 연산 에러율은 수 퍼센트에 이르고 있어서 에러율을 낮추어야 하고, 이를 보정하기 위한 양자에러정정 기술, 고전데이터의 효율적 양자데이터 변환 기술, 양자의 이점을 활용할 수 있는 다양한 양자알고리즘, SW 툴체인, 관측붕괴에 의한 디버깅 불가 극복방법 등이다. 또한, '궁극적인 양자컴퓨터'(아마도 수천 큐빗의 논리큐빗과 양자메모리를 갖춘)를 개발하기까지 시간표와 로드맵 제시도 어렵고, 이러한 도전이 성공하리라는 보장이 없음을 인정하지만, 다음과 같은 노력을 통해 진전을 이룰 수 있을 것을 말하고 있다. 기

술혁신 속도에 영향을 줄 수 있는 요인을 분석, 기술진행상황을 모니터링할 수 있는 평가지표개발, 아이디어와 인력을 공유할 수 있는 개방형 연구개발 생태계 구축(전산, 수학, 물리, 화학, 재료 등 여러 과학분야의 통합 포함), NISQ 양자컴퓨터의 상업화 성공을 이룩하기 위한 상용 SW 개발과 응용성 증명을 통한 성과 입증 등이다. 그러나, 현재의 양자컴퓨터는 에러에 자유롭지 못하므로 실제 계산결과의 신뢰도가 낮아서 상업적 성공 여부에 대해 많은 우려가 있고, John Preskill 교수가 내준 2017년도 숙제였던 슈퍼컴퓨터보다 빠르다는 것을 보여주는 '양자우월성' 증명도 아직 인정받지 못하고 있다. 또한, 암호해독을 우려한 정보보호 분야에서는 양자컴퓨터에서도 안전한(Quantum-Safe) 암호(PQC: Post-Quantum Cryptography)를 개발하고 있고 표준 제정으로까지 이어지고 있는데, 암호표준을 제정하는 NIST(National Institute of Standards and Technology)에서 2019년 1월 PQC 표준기술 2차 후보 기술을 발표[40]하는 등 속도를 내고 있는 상황이다. 따라서, 지금부터 양자컴퓨터의 응용분야를 확장하고 유용성을 밝혀내지 않으면 많은 시간과 자원을 들여 어렵게 완성되어도 응용 가능성이 없어서 사장될 수도 있다는 것을 솔직하게 말하고 있다.

V. 양자센서 기술 동향

1. 양자센서 기술 현황

양자자기장센서, 양자중력센서, 양자이미징이 미국, 중국, 유럽 등에서 연구되고 있다. 양자센서는 C. W. Helstrom[41]이 1969년에 랜덤잡음 속에서 신호검출을 위한 통계적 판단이론의 양자역학적 해석과 밀도연산에 의한 양자적 추정방법 등에 대한 이론으로 양자 시스템에서 센싱 가능함을 보였다. 그러나, 실 양자시스템은 2010년 이후에나 사용 가능해졌고 대부분의 양자센서가 실험실에서 연구 중에 있다. 다만, 자기장센서와 중력센서는 의료분야 적용과 GPS(Global Positioning System) 대체의 유용성 때문에 일부 분야에서는 상업적으로 이용되고 있다. (그림 1)에는 영국 버

(그림 1) 영국 양자센서허브의 업종별 참여 기업 현황[42]

밍엄 대학의 양자센서허브[42]에 참여하는 기업 현황을 보여주고 있는데, 전통적으로 센서가 필요한 업체들 참여가 많은 만큼 새로운 양자센서에 대한 니즈를 알 수 있다.

2. 양자센서 기술 전망

양자자기장센서, 양자중력센서는 미국, 중국에서 GPS를 대신할 양자네비게이션 기술로 주목받고 있고, 미해군연구소 등 국방관련 분야에서 연구가 진행되고 있어서 국방분야에 활용될 것으로 예측된다. 관성항법장치에 의존할 수밖에 없는 핵잠수함의 경우 양자네비게이션 장치를 사용하게 되면 100일 동안 수면 위로 떠오르지 않고 운행하여도 수백 미터 정도 오차범위 내에서 위치확인이 가능하다고 한다[11]. 향후, 단순 센싱을 넘어서서 차세대 양자기술로 발전하여 국방, 자원, 헬스케어, 토목 등 기존 기술과 융합하여 응용될 것으로 전망되는데, 스텔스 전투기를 잡아낼 양자레이다, 자율주행을 위한 양자라이다 등의 미래 양자기술로 발전해갈 것으로 전망된다.

VI. 결론

양자통신의 양자암호통신 분야에서 비록 BB84에 기반한 양자암호통신에 국한하지만, 암호통신 서비스까지 전개되어 ICT 기술로서는 최종 밸류체인 단계인 서비스 단계에 이르게 되었다. 또한, 양자컴퓨터는 20큐빗 이하급의 초기 시제품이지만 상용서비스를 시작하여 고객을 확보해 나가고 있는 상태이다. 반면, 양자센서는 대부분이 아직 실험실에서 연구개발 중인 단계이나 군사목적이나 시장성이 높은 품목 위주로 경쟁적으로 기술개발이 진행되고 있어서 조만간 상용 시제품까지도 가능할 것으로 보인다. 이러한 초기 시제품에 대한 성공은 1990년대부터 20여 년 이상 장기적인 지원과 꾸준한 연구개발의 결과로 생각된다. 비록, 궁극적인 목표인 양자인터넷, 양자메모리를 갖는 결함허용 양자컴퓨터, 양자센서네트워크 등으로 발전하기 위해서는 어떠한 기술적 난관이 있을지 아무도 모르고 얼마나 시간이 걸릴지도 알 수 없지만, 기술혁신을 이끌어내기 위해서 꾸준한 지원과 연구자들의 중단 없는 노력이 필요할 것이다.

반면, 국내는 출발이 늦었다고 볼 수는 없었지만, 현재 상태로는 인력, 연구역량, 연구시설 등에서 선진국에 비해 뒤처져 있다. IITP가 2018년 2월에 발행한 ICT 기술수준조사보고서[43]를 보면, 최고기술보유국인 미국에 비해 기술력 73%, 기술격차 4년으로 ICT 기술 전체 평균인 80.5%, 1.5년에 비해 크게 뒤지고 있다. 국내 양자분야를 여러 가지 측면에서 살펴본 결과 이러한 이유에는 여러 가지 원인이 있겠지만, 발전전망을 볼 때 현재의 초기 시제품 이후 다음 단계의 시제품까지는 상당한 시일이 걸릴 것으로 생각되므로, 국내에서도 방향성을 잘 확립하고 규모 있는 연구비 지원과 연구역량을 강화해 나간다면 충분히 선진국과 동등한 수준까지도 올라갈 수 있을 것이다.

용어해설

BB84 단일광자의 복제불가, 양자난수 등의 성질을 이용하여 두 지점 간 도청의 염려 없이 안전하게 대칭키를 만들어서 서로 가질 수 있는 양자암호분배 프로토콜

약어 정리

ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System
ISG	Industry Specification Group
NISQ	Noise Intermediate-Scale Quantum
NIST	National Institute of Standards and Technology
OTP	One Time Password
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
SNR	Signal-to-Noise Ratio
VPN	Virtual Private Network

참고문헌

[1] https://quantumxc.com

[2] https://quantumexperience.ng.bluemix.net/qx/experience

[3] https://www.research.ibm.com/ibm-q/system-one/

[4] IITP, "ICT R&D 기술로드맵 2023 발표," 2018.12.20., https://www.iitp.kr/kr/1/notice/reportAndClarify/view.it?ArticleIdx=3437&count=true

[5] NSTC, "A Federal Vision for Quantum Information Science," 2008.12.

[6] NSTC, "Advancing Quantum Information Science: National Challenges and Opportunities," 2016.07.22.

[7] NSTC, "National Strategic Overview for Quantum Informaiton Science," 2018.09. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf

[8] US Congress, "H.R.6227-National Quantum Initiative Act." https://www.congress.gov/bill/115th-congress/house-bill/6227/amendments?q=%7B%22search%22%3A%5B%22quantum%22%5D%7D&r=3&s=1

[9] EU Digital Single Market, "EU Funded Project on Quantum Technology." https://ec.europa.eu/digital-single-market/en/projects-quantum-technology

[10] Gov.UK, "New Funding puts UK at the forefront of cutting edge quantum technologies," 2018.11.01. https://www.gov.uk/government/news/new-funding-puts-uk-at-the-forefront-of-cutting-edge-quantum-technologies

[11] South China Morning Post, "China building world's biggest quantum research facility," 2017.09.11., https://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility#comments

[12] 科学技術振興機構, "光・量子飛躍フラッグシッププログラム(Q-LEAP)," https://www.jst.go.jp/stpp/q-leap/index.html

[13] 総務省 国際戦略局, "衛星通信における量子暗号技術の研究開発," https://www8.cao.go.jp/space/comittee/dai66/siryou1-5-6.pdf

[14] The Jerusalem Post, "ISRAEL JOINS THE RACE TO BECOME A QUANTUM SUPERPOWER," 2018.12.17. https://www.jpost.com/Israel-News/Israel-joins-the-race-to-become-a-quantum-superpower-574510

[15] The Print, "India sets off on pursuit of quantum computers, the 'holy grail' of modern tech," 2019.01.14. https://theprint.in/science/india-sets-off-on-pursuit-of-quantum-computers-the-holy-grail-of-modern-tech/175870/amp/

[16] National Cyber Security Centre, "Whitepaper - Quantum key distribution," 2016.10.04. https://www.ncsc.gov.uk/whitepaper/quantum-key-distribution

[17] T.H. Shake et al., "Security performance of optical CDMA Against eavesdropping," Journal of Lightwave Technology, vol. 23, issue: 2, 2005, pp. 655 - 670.

[18] A. Vakhitov et al., "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," J. Mod. Opt., vol. 48, no. 13, 2001, 2023-2038.

[19] N. Gisin et al., "Trojan-horse attacks on quantum-key-distribution systems," Phys. Rev. A, vol. 73, 2006, 022320.

[20] C.-H. Fung et al., "Security proof of quantum key distribution with detection efficiency mismatch," Quant. Inf. Comp., vol. 9, 2009, 131-165.

[21] L. Lydersen et al., "ECURITY OF QUANTUM KEY DISTRIBUTION WITH BIT AND BASIS DEPENDENT DETECTOR FLAWS," Quant. Inf. Comp., vol. 10, 2010, 0060-0076.

[22] Ø. Marøy et al., "Security of quantum key distribution with arbitrary individual imperfections," Phys. Rev. A, vol. 82, 2010, 032337.

[23] L. Lydersen et al., "Secure gated detection scheme for quantum cryptography," Phys. Rev. A, vol. 83, 2011, 032306.

[24] D. Gottesman et al., "Security of Quantum Key Distribution with Imperfect Devices," Quant. Inf. Comp., vol. 4, 2004, 325-360.

[25] H. Inamori et al., "Unconditional security of practical quantum key distribution," Eur. Phys. J. D, vol. 41, 2007, 599-627.

[26] Z. Yuan et al., "Avoiding the blinding attack in QKD," Nature Photonics, vol. 4, 2010, 800-801.

[27] M. Lucamarini et al., "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature, vol. 557, 2018, 400-403.

[28] X.-B. Wang et al., "Effective Eavesdropping to Twin-Field Quantum Key Distribution," arXiv:1805.02272, 2018.05.06.

[29] M. Sasaki, "Quantum networks: where should we be heading?," Quantum Sci. Technol., vol. 2, 2017, 020501.

[30] Quantum Computing Report, "Qubit Count," https://quantumcomputingreport.com/scorecards/qubit-count/

[31] Rigetti, "Quantum Cloud Services opens in public beta," 2019.01.31. https://medium.com/rigetti/quantum-cloud-services-opens-in-public-beta-31989e15e36e

[32] Rigetti, "Better quantum chips," 2019.01.25. https://medium.com/rigetti/better-quantum-chips-52c4dfe4ce64

[33] D-Wave, "D-Wave Launches Leap, the First Real-Time Quantum Application Environment," 2018.10.04. https://www.dwavesys.com/press-releases/d-wave-launches-leap-first-real-time-quantum-application-environment

[34] IonQ, "Request Access," 2019.1. https://ionq.co/request-access

[35] CAS-Alibaba, "Quantum Computing Cloud Accessed," http://quantumcomputer.ac.cn/index.html

[36] U. Bristol, "Quantum in the Cloud," http://cnotmz.appspot.com

[37] J. Preskill, "Quantum Computing in the NISQ era and beyond," arXiv:1801.00862, 2018.01.27., 2018.07.31.

[38] E. Tang, "A quantum-inspired classical algorithm for recommendation systems," arXiv:1807.04271, 2018.07.13.

[39] National Academies of SEM, "Quantum Computing: Progress and Prospects," National Academies Press, 2018.12., ISBN 978-0-309-47969-1.

[40] CSRC, "PQC Standardization Process: Second Round Candidate Announcement," 2019.01.30. https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates

[41] C. W. Helstrom, "Quantum Detection and Estimation Theory," J. Stat. Phys., vol. 1, no. 2, 1969, 231-252.

[42] UK National Quantum Technology Hub - Sensors and Metrology, https://www.quantumsensors.org.

[43] IITP, "2017년도 전문가 심층 인터뷰(FGI)를 통한 ICT 기술수준조사보고서," 2018.2.