

제115회 한림원탁토론회

ICT 패러다임을 바꿀 양자통신, 양자컴퓨터의 부상

2017년 8월 18일(금), 09:30

한국프레스센터 20층 프레스클럽




2017 한국과학주간

Korea Science Week 2017

과학기술 분야 민간외교 확대를 위해 노력해 온 우리 한국과학기술한림원은 올해 전 세계 과학자들과 국내 석학뿐 아니라 신진연구자들과 이공계 학생, 일반대중들까지 참여하는 열린 행사를 마련합니다. 오는 10월 30일(월)부터 11월 1일(수)을 'Korea Science Week 2017'로 명명하고, 노벨과학상 수상자를 비롯해 국내외 세계적인 석학들을 대거 초청, 자유롭고 혁신적인 교류와 토론의 장을 마련하여 우리나라 과학문화 발전에 기여하고자 합니다.

Ⅰ 행사 개요 Ⅰ

행사명	  		
일 시	10.30(월)	10.31(화)~11.1(수)	11.1(수)
장 소	코엑스	더플라자 호텔	
주 제	The Age to Come	Science and Technology in Health Care	Next Revolution for Better Living
주요인사	노벨상 수상자 5인 등 세계적 석학 30여명	각국 한림원 대표단 및 세계적 석학 30여명	젊은 석학 2인 및 Y-KAST 회원 70여명
특 징	발전적이고 융합적인 석학대담회	과학기술 이슈와 정책적 대안 제시	젊은 과학자가 제안하는 과학기술의 미래

한국과학주간(Korea Science Week) 공식홈페이지 www.KoreaScienceWeek.org 와 한국과학기술한림원 홈페이지 www.kast.or.kr 를 통해 각 행사별 홈페이지로 방문이 가능하며, 각 홈페이지 상에서 행사별 일정과 연사, 주제 등 세부 내용을 확인 할 수 있습니다. 모든 행사는 9~10월 홈페이지를 통해 참가 신청을 접수할 예정입니다.

한국과학기술한림원 공식홈페이지



한국과학주간 공식홈페이지



※ 휴대전화에서 QR코드 애플리케이션을 활용하시면 공식 홈페이지로 바로 연결됩니다.

Nobel Prize Dialogue Seoul 2017

한림원과 스웨덴 노벨미디어(Nobel Media)가 공동 개최하는 ‘노벨프라이즈 다이얼로그 서울’은 노벨과학상 수상자 5명을 비롯해 30여명의 세계적인 석학들이 인류의 현황과 미래에 대해 대담하는 과학행사로, 스웨덴에서 노벨상 시상식 주간에 개최되는 ‘노벨위크 다이얼로그(Nobel Week Dialogue)’와 동일한 형태다.

올해 서울에서 개최하는 이번 행사는 ‘The Age to Come’을 주제로, 우리가 곧 마주할 고통사회를 과학뿐만 아니라 사회, 문화 그리고 철학적인 관점에서 탐구해 볼 예정이다.

참가신청은 행사 개최 한 달 전부터 온라인 홈페이지를 통해 받을 예정이며, 접수 비용은 무료다. 행사는 전일 진행되며, 청중들에게는 동시통역 서비스와 가벼운 점심이 제공된다.



Nobel Week Dialogue 2013 ©Bengt Oberger

2017 세계과학한림원서울포럼 (Inter-Academy Seoul Science Forum 2017)

올해 6회를 맞이하는 IASSF는 한림원의 대표적인 국제행사로서 저명한 연구자뿐 아니라 각국의 과학기술계 리더들이 참여해 세계적인 과학기술 이슈와 정책 등을 논의한다. 한림원대표단회의(Inter-Academy Plenary Panel)와 병행세션 등이 마련되며, 각국 한림원 대표단이 참여한 패널 토론을 비롯해 기초과학 분야 국내외 우수과학자들의 최신 연구성과 발표가 진행될 예정이다. 특히 올해는 독일, 폴란드, 싱가포르, 호주, 캐나다 등 7개국의 한림원 대표단이 이번 행사의 주제인 헬스케어 분야와 젊은 과학자 지원(Support for Young Scientists)을 주제로 심도 깊은 토론을 진행할 계획이다.

또한 지난해부터는 국제적인 학술지에 논문을 게재한 잠재력 높은 젊은 과학자 그룹을 초청해서 석학들의 연구발표를 직접 듣고 이야기를 나누는 기회를 제공한다.



2016년 IASSF 행사 전경 ©한국과학기술한림원

Young Scientists Talk 2017

더 나은 삶을 위한 새로운 혁명(Next Revolution for Better Living)’을 주제로 열리는 이번 행사는 지난 2월 말 출범한 한국차세대과학기술한림원 (Young Korean Academy of Science and Technology, 이하 Y-KAST)의 첫 대규모 국제행사로서 차세대회원 73명이 한자리에 모여 소통하고 교류하는 Y-KAST 총회이자, 미래 과학기술을 위한 젊은 과학자들의 생각과 의견을 제안하는 연구정책 국제포럼으로 개최될 예정이다.

행사는 기초강연, 그룹토론, 패널토론, 스케치세션 등으로 나뉘어 진행하며, 오전의 그룹토론에서는 차세대 회원들이 융합(Convergence), 창의 (Creativity), 미래(Future) 등 다양한 주제로 각자가 그리는 미래비전에 대한 스케치(sketch)를 발표하는 자리가 마련된다.



2017년 한국차세대과학기술한림원 출범식 ©한국과학기술한림원

제115회 한림원탁토론회

ICT 패러다임을 바꿀 양자통신, 양자컴퓨터의 부상

2017년 8월 18일(금), 09:30

한국프레스센터 20층 프레스클럽





초대의 말씀

양자통신과 양자컴퓨터 기술은 기존의 정보통신기술에 일대 혁명을 가져올 차세대 핵심 기반기술로써 동 산업에 거는 기대와 희망은 이미 전 세계 각국의 초미의 관심사가 되고 있습니다.

지난해 양자암호통신 위성 발사 성공에 이어 최근에는 이 위성을 이용해 미래 양자통신의 핵심기술 실험(장거리 양자 얽힘 실험)에 성공한 중국의 양자기술이 현재 전 세계적으로 큰 주목을 받고 있는가 하면, 미국, 일본, 유럽 등의 선진국 역시 연간 1조원 이상의 예산을 투입하고 있거나 그에 준하는 대규모 투자계획을 밝히고 있는 실정입니다.

우리나라도 양자산업이 국가의 새로운 미래 성장동력이 될 것으로 예측하며, 문재인 정부 국정운영 5개년 계획에 양자정보통신 육성 방안이 포함되는 등 세계적 기술발전 추이에 뒤지지 않기 위해 비교적 발빠르게 움직이고 있습니다.

국내 산업계에서는 이미 일부 통신사업자 등을 중심으로 양자암호통신에 대한 투자환경을 마련하고 있지만, 동 기술분야에 대한 글로벌 주도권을 확보하기 위해서는 정부의 역할이 그 어느 때보다 중요하다 할 것입니다.

이번 토론회는 정보통신기술의 차세대 핵심 기반기술로써의 양자통신과 양자컴퓨터에 대해 국내 최고의 전문가 분들을 모시고 향후 발전방안을 비롯한 관련분야의 생태계 조성 등에 대해 다양한 의견과 지식을 공유하는 자리가 될 것입니다.

바쁘시더라도 'ICT 패러다임을 바꿀 양자통신, 양자컴퓨터의 부상'을 주제로 개최되는 제115회 한림원탁토론회에 많이 참석하시어 고견을 개진해 주시기 바랍니다.

감사합니다.

2017년 8월
한국과학기술한림원 원장 이 명 철

한림원탁토론회는 국가 과학기술의 장기적인 비전과 발전전략을 마련하고 국가사회 현안문제에 대한 과학기술적 접근 및 해결방안을 도출하기 위해 개최되고 있습니다.

PROGRAM

제115회 한림원탁토론회 'ICT 패러다임을 바꿀 양자통신, 양자컴퓨터의 부상'

사회: 유욱준 한림원 총괄부원장

- | | |
|------------------|---|
| 09:00~09:30(30') | 등 록 |
| 09:30~09:40(10') | 개회사

이명철 한국과학기술한림원 원장 |
| 09:40~09:45(05') | 인사말

강성주 과학기술정보통신부 정보통신산업정책관 |
| 09:45~09:50(05') | 기념촬영 |
| 09:50~10:50(60') | 세부발제 [기술현황 및 미래전망]

세부발제 1 <양자통신 및 암호> '양자통신 국내외 기술현황 및 전망'
허 준 교수(고려대학교 스마트양자통신센터장)

세부발제 2 <양자컴퓨터> '양자컴퓨터'
최병수 박사(한국전자통신연구원 양자창의연구실장)

세부발제 3 <실용화 및 상용화> '양자암호통신 및 양자컴퓨터의
실용화/상용화 전망'
김태현 박사(SK텔레콤 퀀텀테크랩) |
| 10:50~11:20(30') | 주 발 제 [R&D 및 산업화 전략]
'양자기술의 국가 R&D 및 산업화 전략'
문성욱 박사(한국과학기술연구원 양자정보연구단장) |

PROGRAM

제115회 한림원탁토론회 'ICT 패러다임을 바꿀 양자통신, 양자컴퓨터의 부상'

11:20~11:30(10') 단상정리 및 휴식

11:30~12:20(50') 지정토론

- 좌 장: 이석한 한림원 학술담당부원장(성균관대학교)
- 토론자: 김길호 교수(성균관대학교)
(가나다 順) 김용주 기자(전자신문)
박성수 박사(한국전자통신연구원 미래연구부장)
백정현 상무((주)EYL)
안도열 석좌교수(서울시립대, (주)페타룩스 대표)

12:20~12:40(20') 청중토론

12:40 폐회 및 오찬

CONTENTS

제115회 한림원탁토론회 'ICT 패러다임을 바꿀 양자통신, 양자컴퓨터의 부상'

I. 세부발제 [기술현황 및 미래전망]

- 세부발제 1. 〈양자통신 및 암호〉 '양자통신 국내외 기술현황 및 전망'
 - 허 준 교수(고려대학교 스마트양자통신센터장) 3
- 세부발제 2. 〈양자컴퓨터〉 '양자컴퓨터'
 - 최병수 박사(한국전자통신연구원 양자창의연구실장) 17
- 세부발제 3. 〈실용화 및 상용화〉 '양자암호통신 및 양자컴퓨터의 실용화/상용화 전망'
 - 김태현 박사(SK텔레콤 퀀텀테크랩) 29

II. 주발제 [R&D 및 산업화 전략] '양자기술의 국가 R&D 및 산업화 전략'

- 문성욱 박사(한국과학기술연구원 양자정보연구단장) 43

III. 지정토론

- 좌 장: 이석한 한림원 학술담당부원장(성균관대학교)
- 토론자
 - 김길호 교수(성균관대학교) 63
 - 김용주 기자(전자신문) 71
 - 박성수 박사(한국전자통신연구원 미래연구부장) 75
 - 백정현 상무((주)EYL) 81
 - 안도열 석좌교수(서울시립대, (주)페타룩스 대표) 89

I . 세부발제

[기술현황 및 미래전망]

발제자 약력

성 명	허 준	
소 속	고려대학교 공과대학 전기전자공학부	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
1985. 3.~1989. 2. 1989. 3.~1991. 2. 1997. 8.~2002. 6.	서울대학교 서울대학교 대학원 University of SouthernCalifornia	전자공학 통신및부호이론 디지털통신 및 부호이론
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
1991. 2.~1995. 12. 2001. 8.~2002. 7. 2003. 3.~2007. 2. 2007. 3.~현재 2006. 3.~현재 2015. 7.~현재 2015. 8.~현재	LG 전자 Trellisware Inc. 건국대학교 고려대학교 한국통신학회 한국통신학회 양자통신연구회 스마트양자통신 ITRC 센터	선임연구원 Senior Engineer 교수 교수 상임이사 위원장 센터장

세부발제 1

'양자통신 국내외 기술현황 및 전망'

허 준

고려대학교 스마트양자통신센터장

양자통신 국내외 기술현황 및 전망

고려대학교
전기전자공학부
스마트양자통신 ITRC센터
허 준

2017.08.18
한림원 원탁 토론회

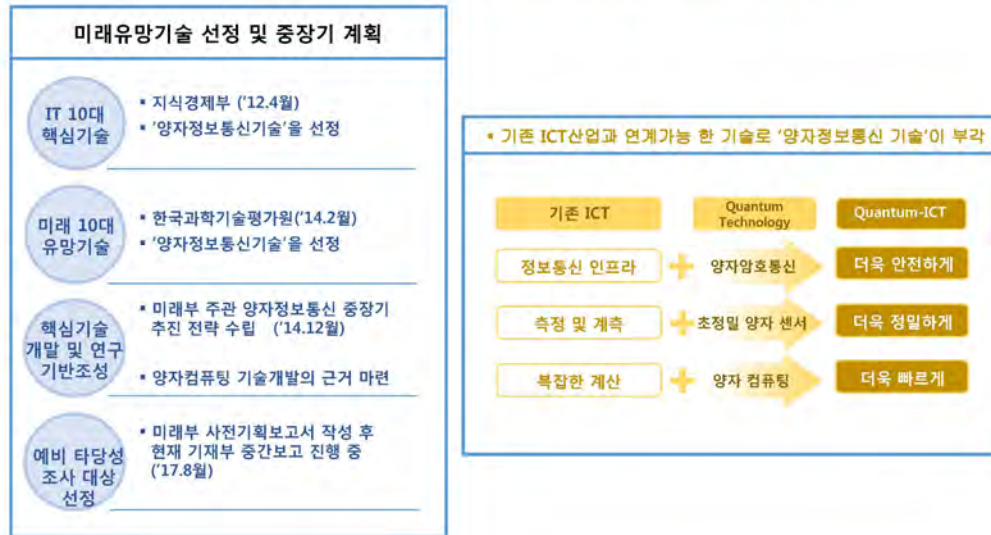
차 례

- 양자통신 용어 정리
- 양자통신 국내외 정책 동향
- 양자통신기술 국내외 개발 동향
- 양자(암호)통신 기술 개요
- 맺음말

양자통신 용어

- 양자 (Quantum)
더 이상 나눌 수 없는 에너지의 최소 단위 (예: Photon 등)
- 양자상태 (Quantum State)
고전역학에서 나타나지 않는 양자 고유의 성질(중첩, 얽힘, 불확정성 등)을 갖는 상태
- 양자정보
양자물리학에 기반하여 양자상태와 양자연산자 등을 수학적으로 묘사하고
공학적으로 구현하는 기술
- 양자(암호)통신
양자물리학에 근거한 암호키 분배 기술로서 도청을 차단할 수 있는 새로운
통신 보안 기술
- 양자컴퓨터
양자정보이론을 이용하여 초고속 연산이 가능한 미래형 특수목적(암호해독,
데이터 검색 등) 컴퓨터

양자정보통신 국내 정책 수립 동향



해외 정책 현황



해외 기술 동향 (양자통신)

 <ul style="list-style-type: none"> ▪ (미국) 항공우주국 ▪ 560Km 거리의 양자암호통신 네트워크 구축 중 ('13년~) 	 <ul style="list-style-type: none"> ▪ (일본) 정보통신연구기구 ▪ 도쿄 양자암호통신 네트워크(JGN2 Plus) 구축 ('10년) ▪ 45Km 거리의 양자암호화 동영상 전송 실험 성공('12년) ▪ 무인 드론 제어용 양자암호통신 실험 성공('16년)
 <ul style="list-style-type: none"> ▪ (미국) MagiQ Technologies社 ▪ 120Km 거리의 양자암호통신 시스템 상용화('03년) ※ MagiQ社의 양자암호 시스템은 수출통제 품목 	 <ul style="list-style-type: none"> ▪ (일본) 전신전화 ▪ 양자메모리가 없는 장거리 양자암호 전송 이론 개발 ('15년)
 <ul style="list-style-type: none"> ▪ (독일) 막스플랑크연구소 ▪ 144Km 거리의 무선 양자암호통신 실험 성공 ('07년) 	 <ul style="list-style-type: none"> ▪ (중국) 중국과학기술 대학(USTC) 등 ▪ 안후이성~베이징 구간 양자암호 시험통신망 구축 ('07년) ▪ 우후(Wuhu)市 행정 업무용 양자암호통신 망 구축('09년) ▪ 2,000Km 구간(베이징~상하이) 양자암호통신 백본망 건설중 ('16년~) ▪ 양자암호통신 위성 발사 성공 ('16. 8.17.)
 <ul style="list-style-type: none"> ▪ (스위스 ID Quantique社) ▪ 세계최초 양자암호통신 상용화 ('02년) ▪ 307Km 구간 1kbps급 양자암호통신 제품 생산('13년) 	<div style="border: 1px solid red; padding: 5px; display: inline-block;">북한</div> <ul style="list-style-type: none"> ▪ (북한) 양자암호통신 기술개발 성공 발표 ('16.1.31)

국내 기술 동향 (양자통신)

기관	일시	내용
ETRI (한국전자통신연구소)	2005.03	Table-top 양자암호 송수신 시스템 시연
고려대학교	2015.08	양자정보통신기술 인력양성 센터 개소 (미래부지원)
SK텔레콤	2016.02	양자암호시험망구축 (분당-용인 68km)
KIST(한국과학기술원)-KT	2017.06	양자통신 응용연구센터 개소

암호의 정의

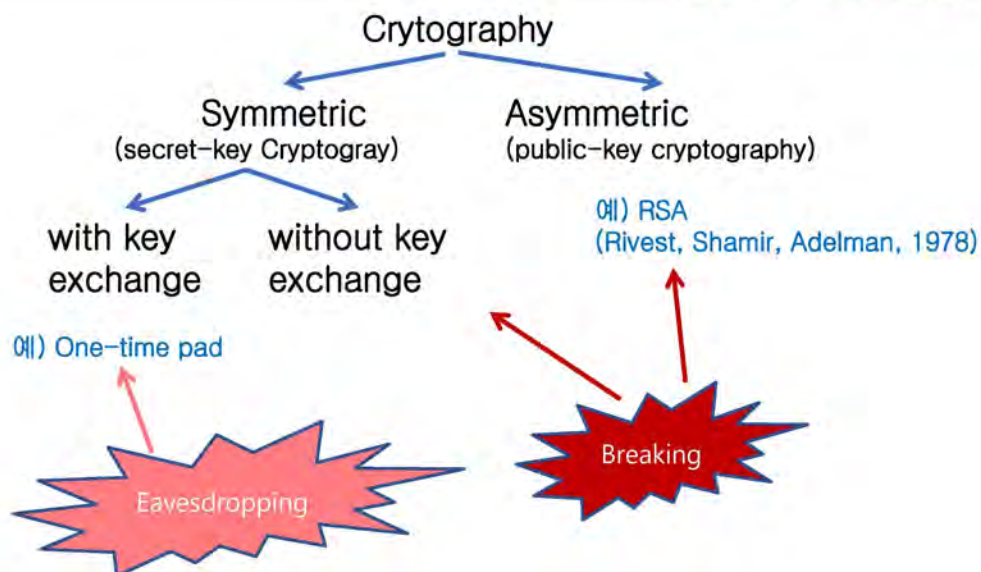
■ 암호 (Cryptography)

- 중간 도청자가 알아볼 수 없도록 하여 한 장소에서 다른 장소로 정보를 전달해 주는 체제
- 그리스어 kryptos (secret) + graphein (writing) = cryptography

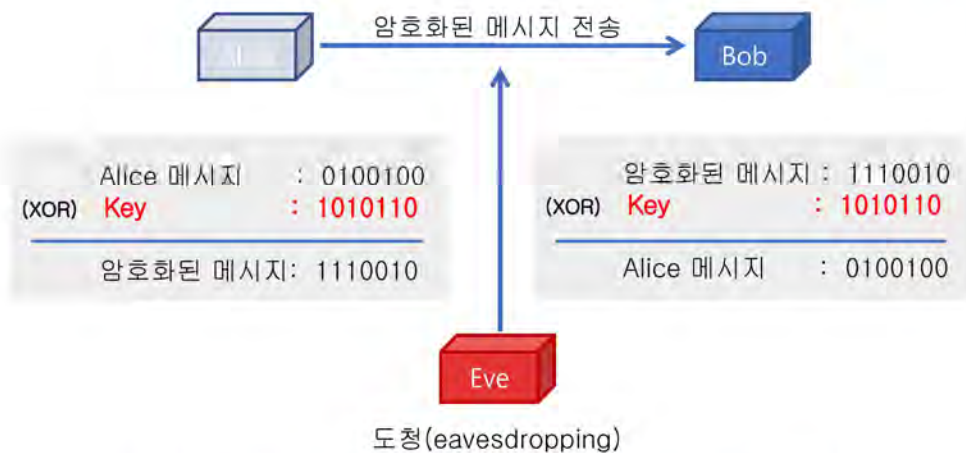
■ 보안이 필요한 정보 예

- 신용카드번호, 개인신상정보 등

암호체계의 분류



Key 분배 문제



암호화 Key 를 안전하게 나누어 갖는 문제가 관건

암호 체계의 위험요소

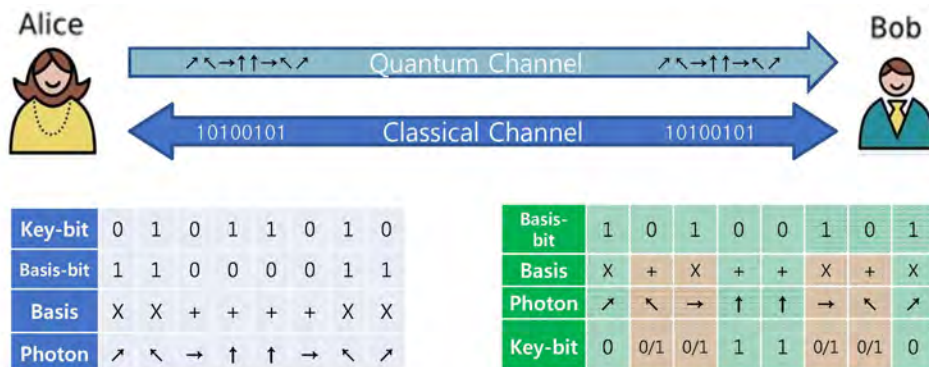
- **RSA (= public key cryptography)**
 - 발생 가능한 key 추정하여 해독함 (key breaking)
 - 매우 큰 소수의 소인수분해는 현재의 컴퓨터로 매우 오랜 계산 시간이 걸림, 따라서 현실적으로 key breaking 이 불가능 함
 - 양자컴퓨터로 매우 큰 소수의 소인수분해가 단시간에 가능한 알고리즘이 개발됨 (Shor algorithm, 1997)
- **One-time pad (secret key cryptography)**
 - key exchange 사이에 발생하는 도청 (eavesdropping)
 - 양자역학을 이용하여 key exchange 사이에 도청이 불가능한 알고리즘 개발 (QKD, since 1984)

양자암호통신(QKD) 시스템 구성도



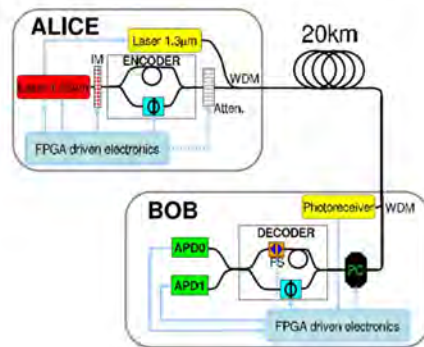
QKD BB84 protocol

Example)



Source of figure - CIS LAB - Quantum Key Distribution Seminar

One-Way Weak Coherent Pulse QKD, Phase Coding



- Attn : attenuator
- IM : intensity modulator
- PC : polarization controller
- WDM : wavelength division multiplexer
- FS : fiber stretcher
- APD : Avalanche Photodiode

Source of Figure : QKD systems Chapter in Lecture Notes in Physics (LNP) - May 2010

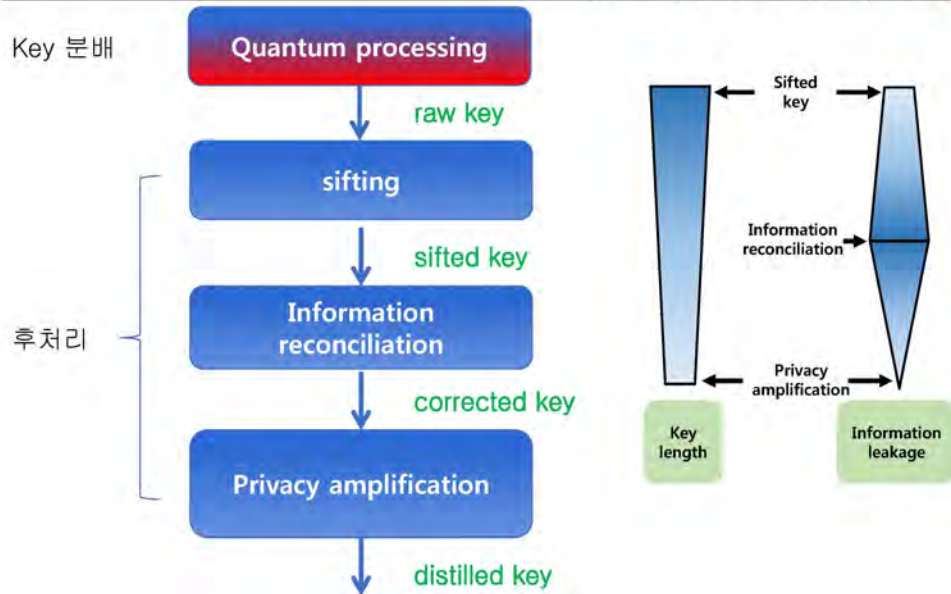
Key 추출 과정



Key 오류율 = Sifted key 의 25% <= 도청 여부 판단 기준

오류정정 한계를 고려하여 Key 오류율이 약 12~13% 이상이면 Raw Key 전송부터 restart

QKD processing step

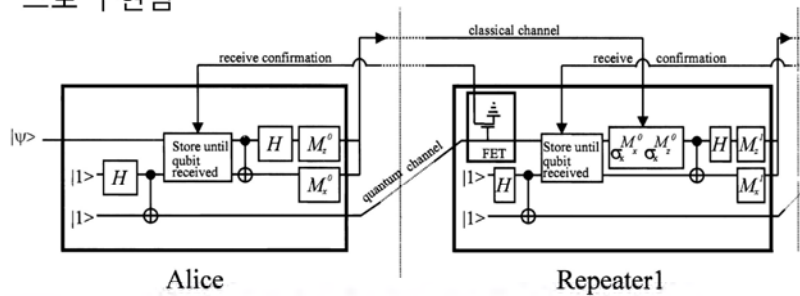


양자 암호 (QKD) 방식의 분류

BB84	E91	Continuous Variable
1984년 Bennette 제안 및 실험	1991년 Ekert 제안	1999년 Ralph 제안
단광자 전송 방식	양자얽힘 이용	연속변수 이용
비교적 간단	복잡	복잡
전송거리 제한 (<30km)	얽힘 양자 발생이 어려움	기존의 광통신 인프라 사용 가능성
전송속도 제한 (<kbps)	고속전송가능 (>Mbps)	
2003년 NEC 전송 실험	2004년 Gisin 50km 전송 실험	2003년 프랑스-벨기에 연구팀 실험

양자중계기(Quantum Repeater)

- 양자상태는 주변의 영향으로 쉽게 훼손되므로 장거리(100km이상) 전송을 위해서는 중계기가 필요함
- 양자중계기는 양자중계기는 한 장소에서 다른 장소로 양자상태를 전송하는 기술로서 **quantum memory**와 **teleportation**기술을 바탕으로 구현됨

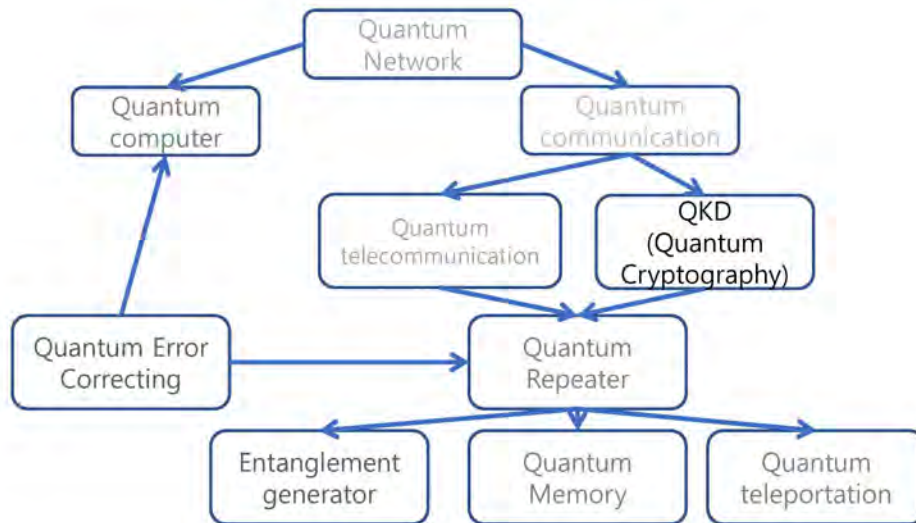


PROCEEDINGS OF THE IEEE, VOL. 91, NO. 5, MAY 2003

양자암호통신 개발 로드맵

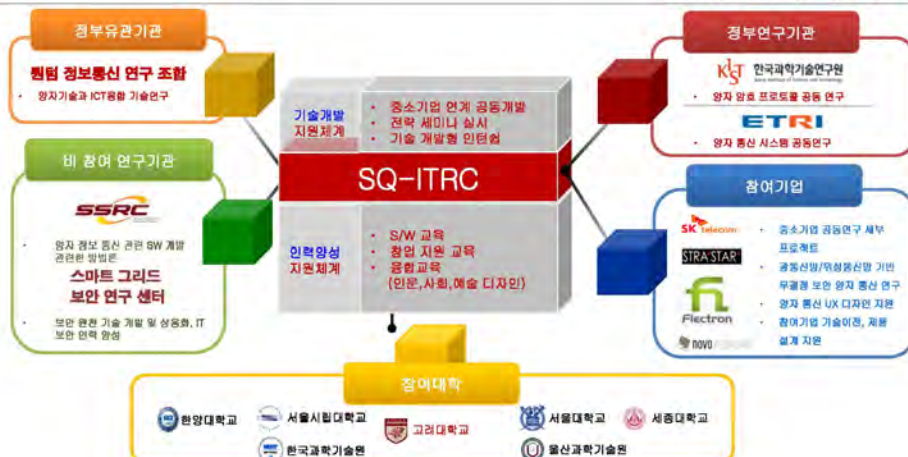
- 2014년 : 범부처 양자정보통신 개발계획 수립
- 2015년 : SKT QKD 시연
- 2016년 : 양자암호 시험통신망 구축 (서울~분당)
- 2018년 : 양자암호 시험통신망 구축 (서울~대전)
- 2018년~2021년 : 무선양자암호통신 기술 개발
- 2021년~2025년 : 유무선 통합 양자암호통신 국가 시험망 구축

양자정보통신 기술 발전 전망



Smart Quantum Communication ITRC

연구센터의 구성



총괄책임	허 준 교수
참여연구진 구성	대학교수 14명, 참여학생 48명, Post-Doc 1명, 산업체 22명
협력기관	총 6개 기관
참여기업	총 4개 업체

Thank You

발제자 약력

성 명	최 병 수	
소 속	한국전자통신연구원 초연결통신연구소 초연결원천연구본부 양자창의연구실	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
1992.3~1996.2	충남대학교	컴퓨터공학 학사
1996.3~1998.2	광주과학기술원	정보통신공학 석사
1998.3~2004.2	광주과학기술원	정보통신공학 박사
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
2004.4~2006.7	영국 요크대학교 전산학과	박사후 연구원 (양자알고리즘)
2006.8~2007.8	성균관대학교 정보통신공학부	박사후 연구원, 연구교수 (양자알고리즘)
2007.9~2010.7	이화여자대학교 정보통신공학부	연구교수 (양자알고리즘, 양자회로, 양자오류보정-결함허용)
2010.9~2011.10	서울시립대학교 양자정보처리연구단	학술연구교수 (양자회로, 양자오류보정)
2011.11~2013.10	미국 듀크대학교 전기컴퓨터공학과	연구원 (양자컴퓨팅시스템설계)
2013.11~2015.5	동경대학교 응용물리학과	연구원 (반도체큐비트블럭)
2015.9~2016.2	한국전자통신연구원 양자창의연구센터	센터장 (양자컴퓨팅 플랫폼 구축)
2016.3~현재	한국전자통신연구원 양자창의연구실	실장 (양자컴퓨팅 플랫폼 구축)

세부발제 2 '양자컴퓨터'

최 병 수

한국전자통신연구원 양자창의연구실장

양자컴퓨터

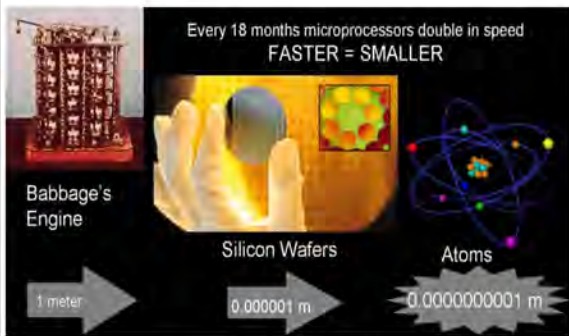
한국전자통신연구원
양자창의연구실
최병수

2017.08.18.

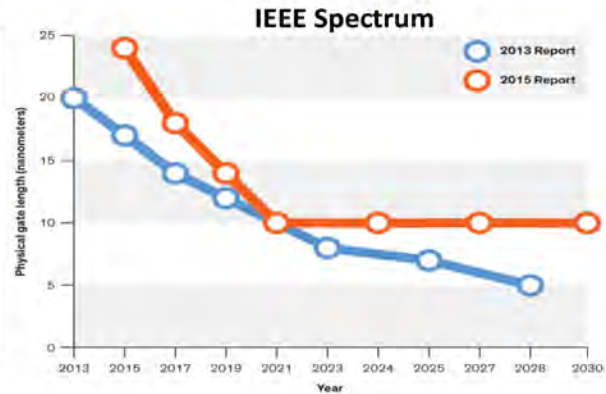
비트의 한계 → 새로운 정보표현방법 필요

- 비트 구현 방법의 지속적 개선과정에서 비트형태 유지 기술의 어려움 증가 → 기술대비비용 증가 발생
→ 경제적 이득 감소 → Moore Stress 현상 발생
→ 고전컴퓨팅의 한계 봉착 (무어 법칙의 공식적 폐기, ITRS 2016)

※ 뉴로모픽 기법도 포스트 무어 컴퓨팅 중 하나이지만, 비트 기반임



<http://www.quantiki.org/wiki/File:Shrinkingcomputer.jpg>



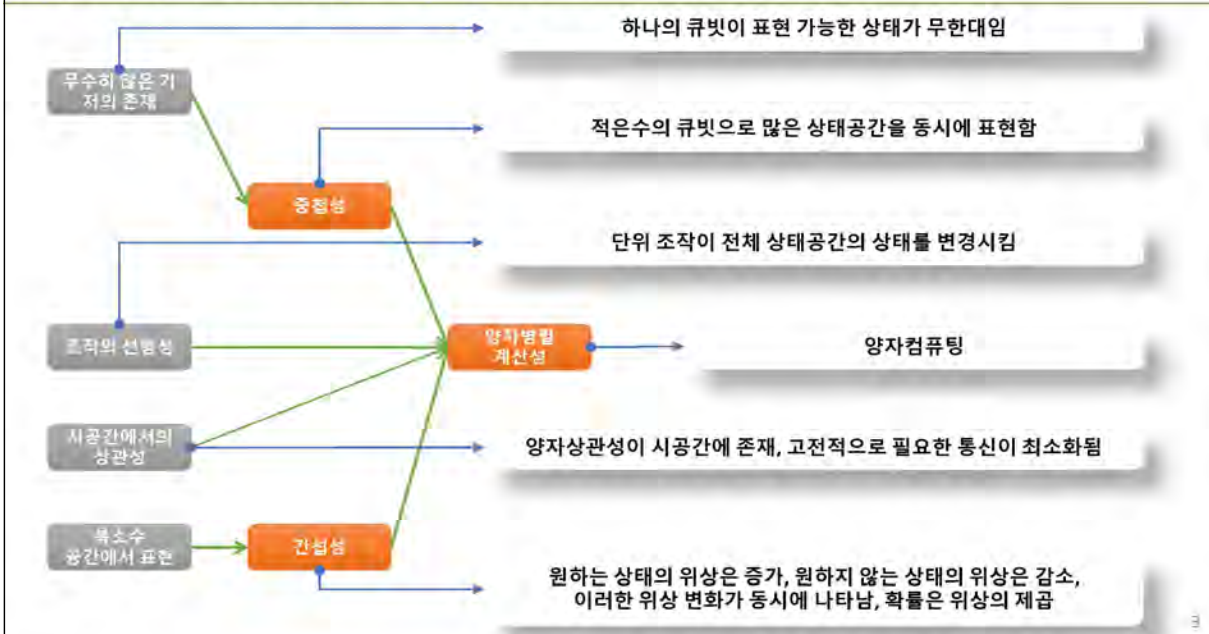
End of The Road: ITRS had previously predicted that the physical gate length of transistors would shrink until at least 2028 [see blue line]. The last ITRS report shows this feature size going flat in the coming years. But ITRS chair Paolo Gargini says that some further scaling may be possible after transistors go vertical.

<http://spectrum.ieee.org/semiconductors/devices/transistors-could-stop-shrinking-in-2021>

2

양자역학 → 양자정보 → 양자컴퓨터의 탄생

- 양자 중첩 특성은 N 개의 상태공간을 $\log N$ 으로 감소(고전컴퓨팅에서 지수적 메모리 공간을 요구함)
- 양자 간섭 특성은 $\log N$ 개의 간섭계로 N 개의 데이터를 연산함
- 양자 얽힘 특성은 공간적으로 떨어진 데이터간 상관관계 가능하게 함(고전컴퓨팅에서 불가능함)
- 양자컴퓨팅은, 고전컴퓨팅에서 어렵거나 불가능한 양자적 특성을 적극적으로 활용함

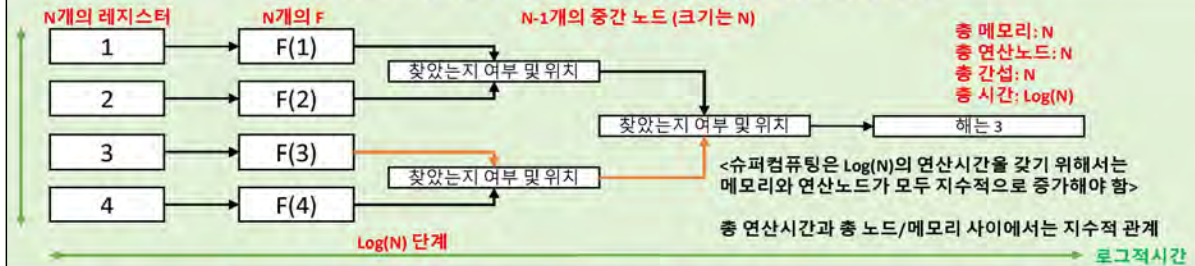


3

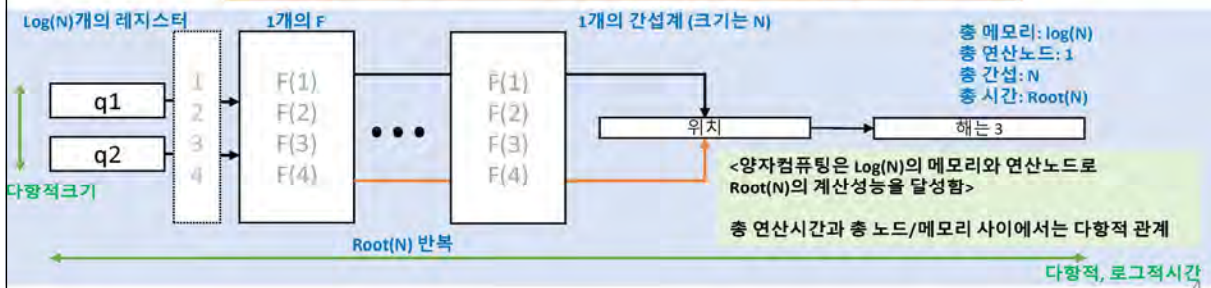
양자컴퓨터의 계산방식

- (비트기반) 슈퍼컴퓨팅은 많은 메모리와 연산노드를 병렬 사용, 병렬성 극대화를 위해 메모리와 연산노드가 지수적 필요
- 양자컴퓨팅은 양자중첩현상 등을 활용, 지수적으로 적은 메모리와 연산노드 사용

<예시: 해결하고자 하는 문제는 탐색 대상 4개에서 $f(x)$ 를 만족하는 x 를 찾기>

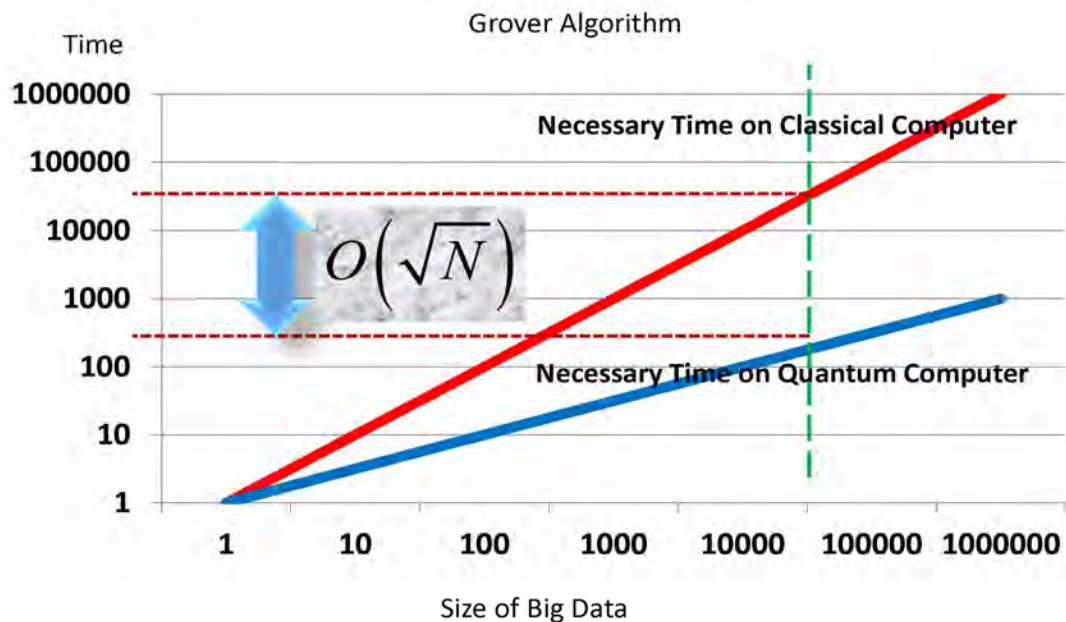


지수적*로그적(슈퍼컴퓨팅) > 다항적*다항적(양자컴퓨팅)



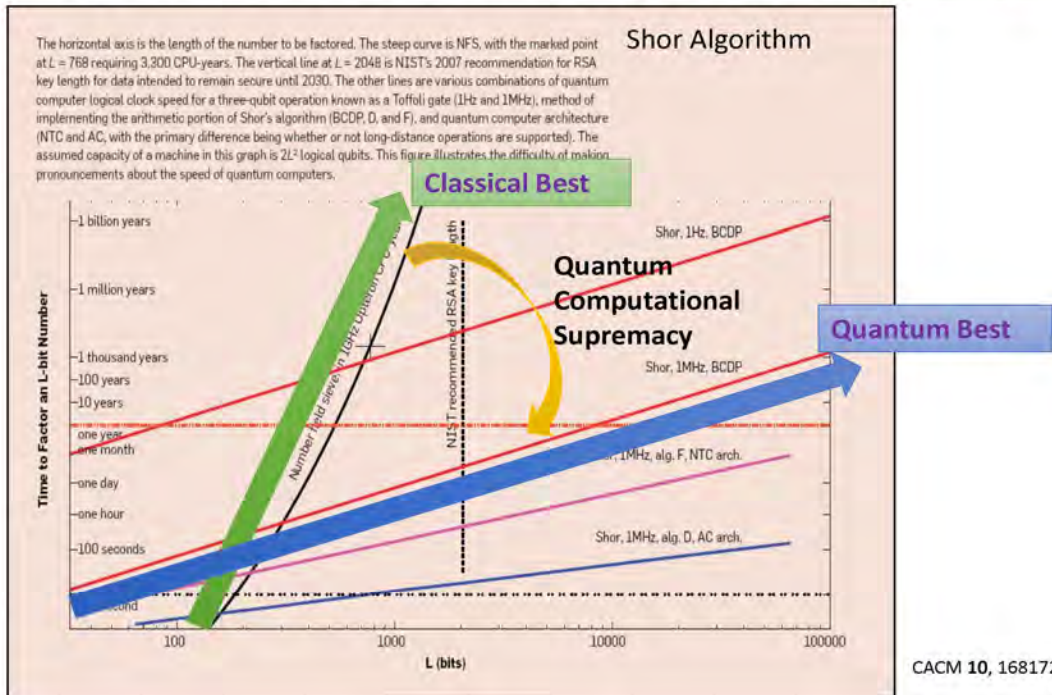
양자컴퓨터의 대표적 위력

- NP-Complete 문제인 임의 탐색 문제의 경우, 양자컴퓨팅도 지수적 성능향상은 불가
- 임의 탐색 문제의 경우, 양자컴퓨팅은 다항적 (quadratic) 속도 향상 효과를 가짐
- 임의 탐색 문제의 범용적 활용가치가 매우 높아서, 양자컴퓨팅의 활용가치도 높음



양자컴퓨터의 대표적 위력

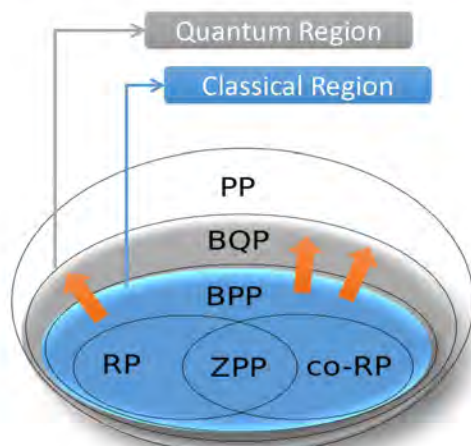
- 공개키 암호체계의 대표적 사례인 “큰 수의 소인수분해” 문제에 대한 고전과 양자 접근법의 차이
- 현재 NIST에서는 RSA 3072이상 권고
- 현재 NIST에서는 양자컴퓨팅 출현 이후에도 안전한 공개키 알고리즘 공모중 (Post-Quantum Cryptography)



6

양자컴퓨팅의 전산학적 의의

- 양자컴퓨팅은 고전컴퓨팅이 수행하는 모든 문제를 해결 가능 (계산효율성과 해결가능성과는 별개)
- 양자컴퓨팅 구현의 초기 단계로 인한 단위 계산 성능이 매우 낮음 (Q ALU Operation 하나가 몇 분 소요)
- 당분간은 고전컴퓨팅이 비용효율적이지만, 일정 시점이 지나면 양자컴퓨팅이 대체
- 문제의 유형에 따라서 (비트기반) 고전컴퓨팅과 양자컴퓨팅의 영역이 구분될 것으로 예상



[http://en.wikipedia.org/wiki/BPP_\(complexity\)](http://en.wikipedia.org/wiki/BPP_(complexity))

BPP: Bounded (Classical) Probabilistic Polynomial Time Complexity,

The Largest Class of Efficiently Solvable Problems on the Classical Machine

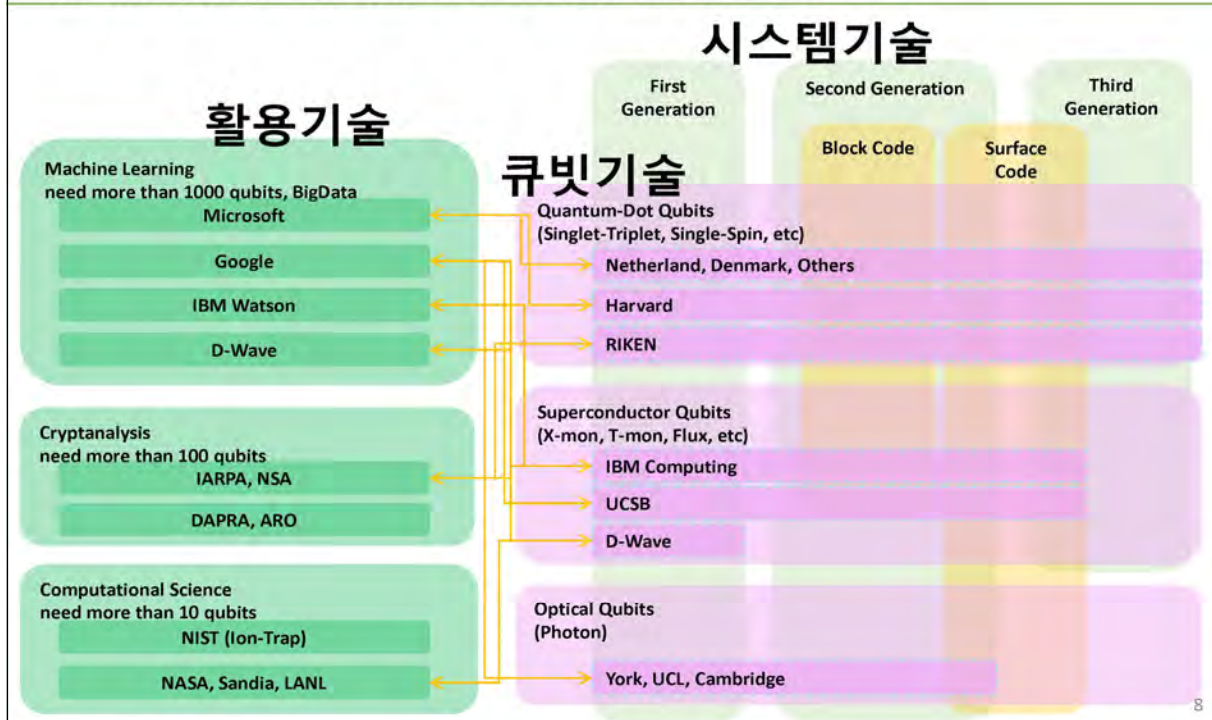
BQP: Bounded Quantum (Probabilistic) Polynomial Time Complexity,

The Largest Class of Efficiently Solvable Problems on the Quantum Machine

7

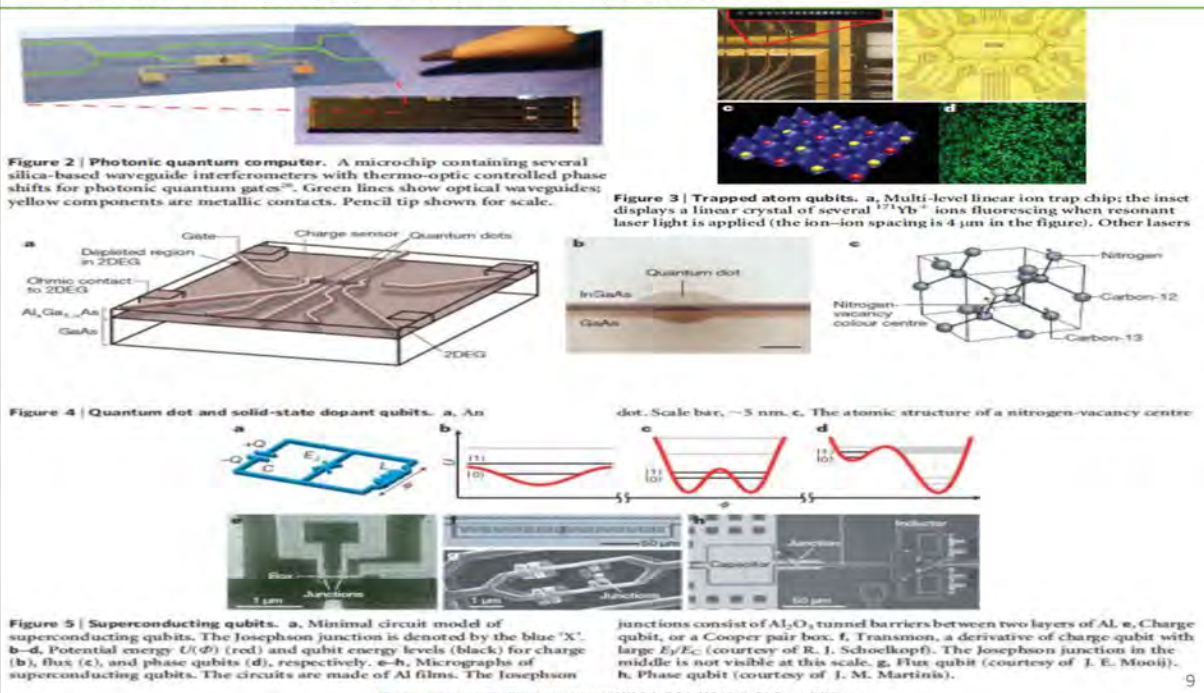
양자컴퓨팅 시스템 구조

- (큐빗기술) 컴퓨팅용 큐빗 및 게이트 구현 가능 기술 필요
- (활용기술) 양자컴퓨팅 활용 알고리즘 기술 필요
- (시스템기술) 양자알고리즘을 양자하드웨어에 연결시키는 시스템 기술 필요



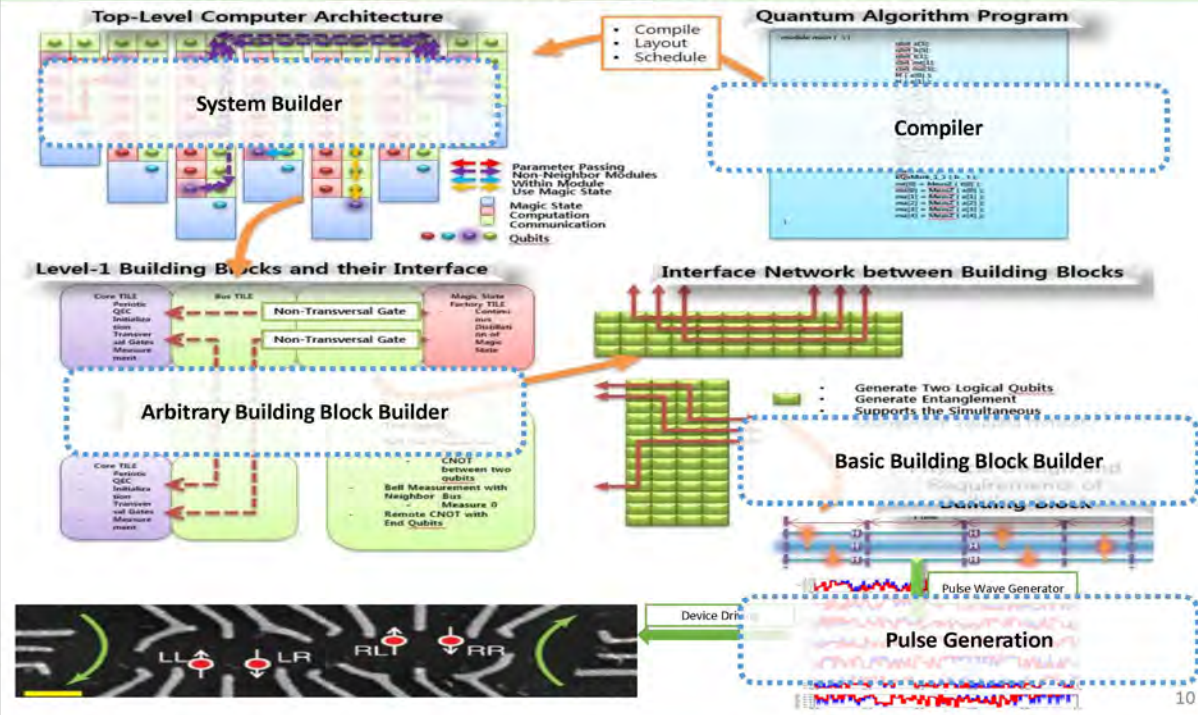
큐빗기술

- 양자상태(예 중첩) 표현 가능해야 함 → 잠재적으로 많은 후보 기술군이 존재
- 양자상태의 초기화, 변환(게이트), 관측 가능해야 함 → 각 기술별로 용이성이 다름
- 다수의 큐빗이 집적가능해야 함 → 각 기술별로 확장성이 다름
- 최적의 큐빗기술은 아직 미정 (초전도, 이온트랩 기술이 현재 가장 선두)



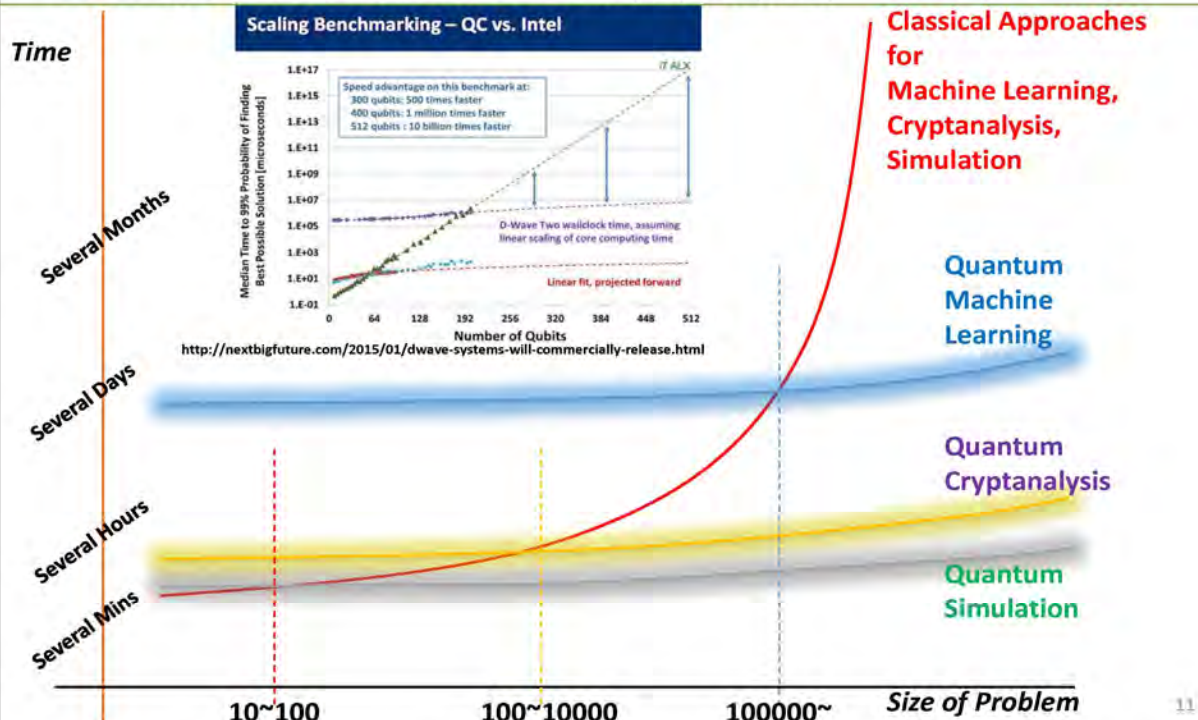
시스템기술

- 사용자 입장에서 프로그래밍 가능해야 함 → 양자프로그래밍 언어 → 컴파일러 → 디버깅 기술 필요
- 하드웨어 기술적 제약사항 반영되어야 함 → 큐비트의 최적배치, 실시간 제어의 중요성, Dead-Lock 회피의 중요성
- 신뢰성, 확장성, 범용성 등 컴퓨팅의 일반적 요구 수준이 충족되어야 함 → 신뢰성 기술이 우선 시급



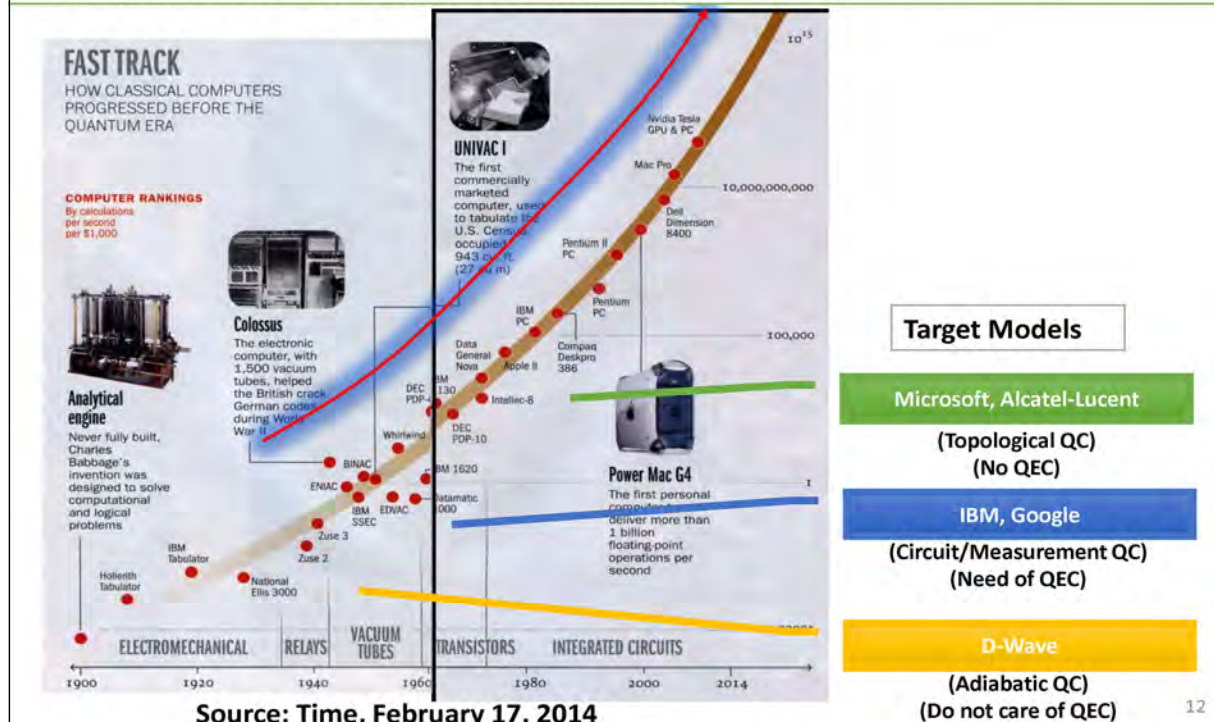
활용기술

- 기존 고전알고리즘의 단순한 양자변환은 무의미, 고전알고리즘대비 성능이 더 우수해야 함
- 양자특화형 기본 연산 엔진은 Q Random Walk, Q Amplitude Amplification, Q Fourier Transform, Q Simulation 등
- 대부분의 활용 알고리즘은 기본 연산 엔진의 부분적 활용 (Shor, Grover, HLL 등)



양자컴퓨팅 모델

- 1세대(아날로그 혹은 비범용성 모델) → 양자컴퓨팅의 실현 가능성 확인 및 일부 실용적 활용 가능 (D-Wave)
- 2세대(디지털 혹은 범용성 모델) → 신뢰성, 확장성, 범용성 기술 적용 → 통상적인 컴퓨팅 수준 기능
- 3세대(디지털 및 새로운 큐비트 모델) → 큐비트 기술에서의 개선 반영



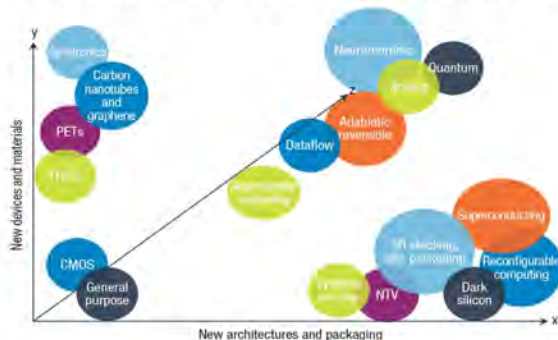
12

양자컴퓨팅 실현의 어려움

- 양자컴퓨팅은 양자정보 실현소자, 양자병렬성 (중첩, 간섭, 얽힘) 활용 알고리즘, 이를 지원하는 컴퓨터 명령어 등 대부분 영역에서 연구개발 필요
- Software와 Hardware의 융합적 접근 필요, Theory와 Practical의 통합적 접근 필요
- Science, Engineering, Business 영역의 혼재

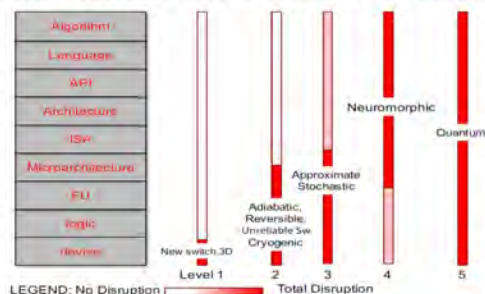
새로운 장치와 새로운 구조/패키징이 요구됨

컴퓨팅 전 영역에서 새로운 접근이 요구됨



IEEE Computer 48(12), 14-23, December 2015

Differing Levels of Disruption in Computing Stack

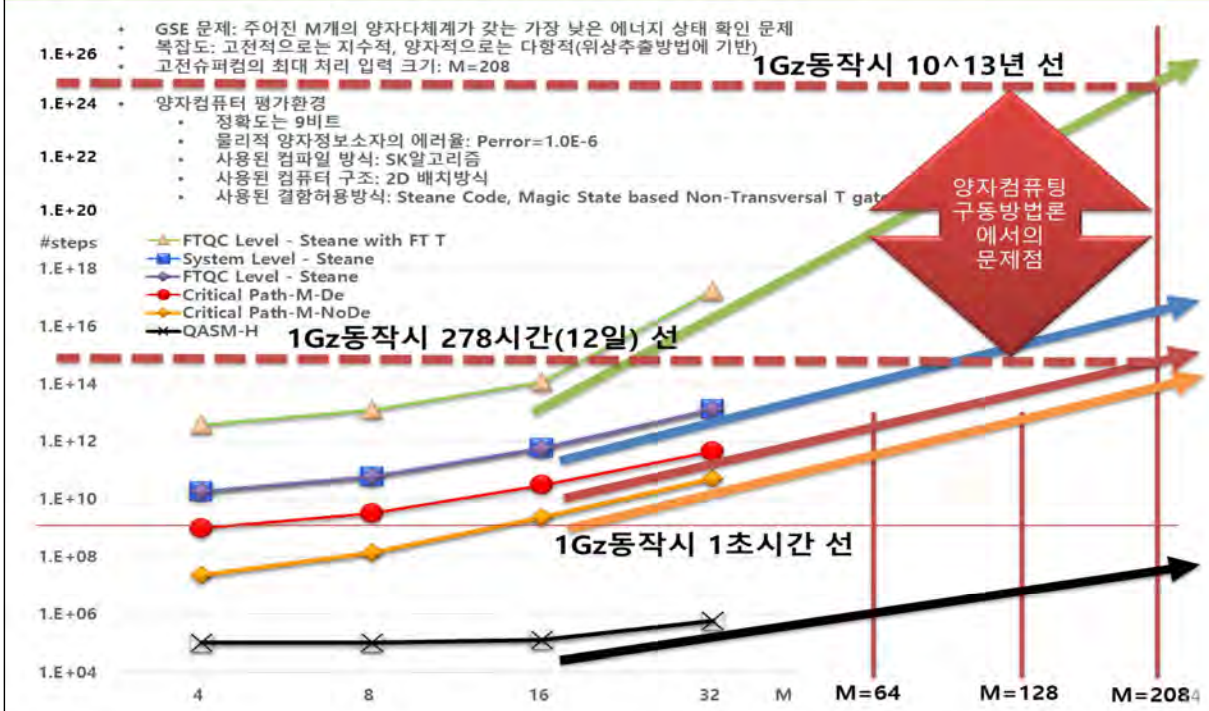


https://arch2030.cs.washington.edu/slides/arch2030_tom_conte.pdf

13

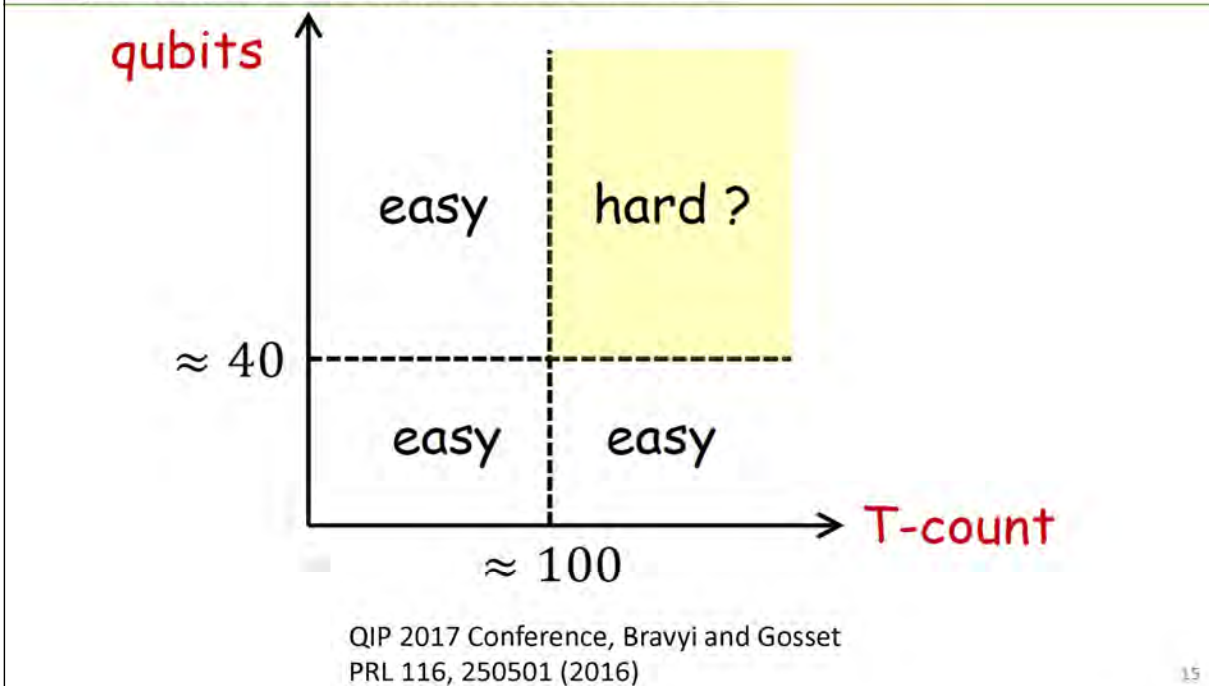
양자컴퓨팅을 넘어 양자슈퍼컴퓨팅으로

- 알고리즘 수준에서의 기대치는 매우 이상적 → 지수적, 다항적 계산성능 향상 가능(단, 복잡도 수준에서)
- 하드웨어 수준에서의 현실치는 매우 현실적 → 절대적 계산시간 측면에서는 현저히 낮은 수준
- 초기 양자컴퓨팅은 기대성능을 달성하기가 쉽지는 않음



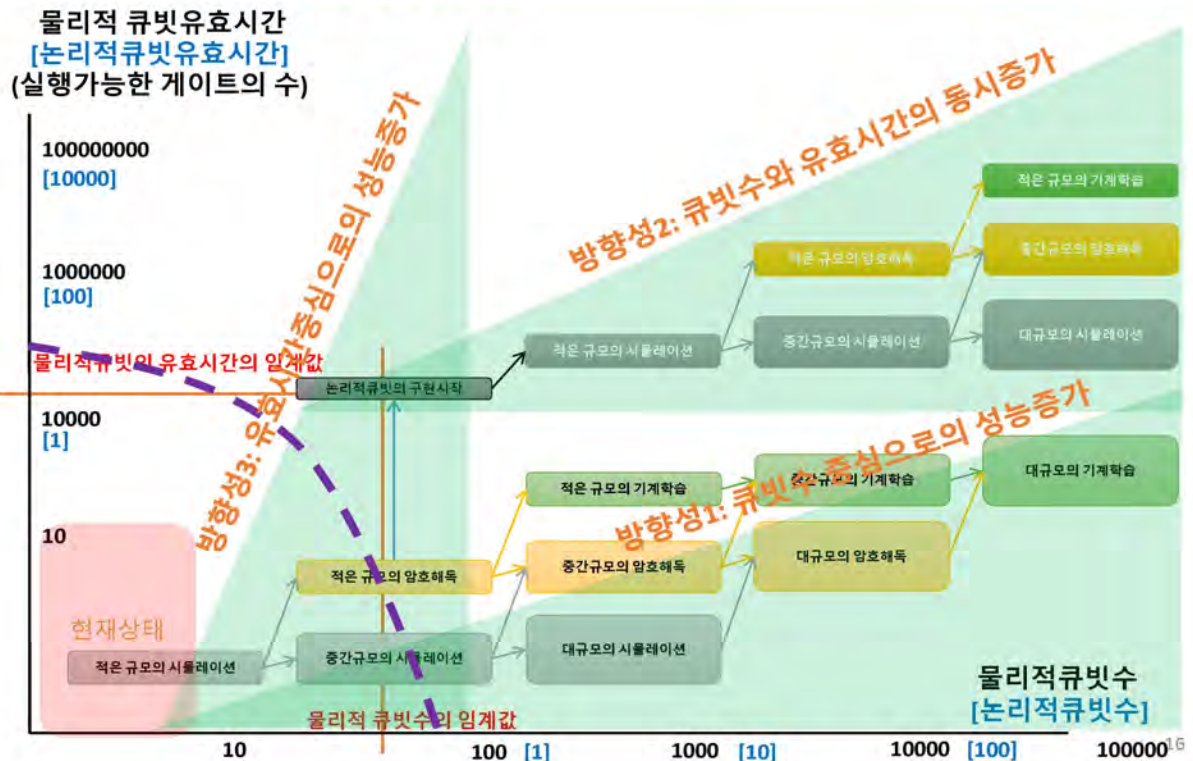
고전적으로는 불가, 양자적으로는 가능한 문제 (임계문제)

- 단계별 접근 필요 → 우선 고전적으로는 불가능하지만, 양자적으로는 용이한 문제를 통해서 우월성 입증 필요
- (신뢰성은 포기하고) 계산측면에서 고전컴퓨팅대비 우월성이 가능함을 확인하는 과정이 필요
 - ※ (통신분야) 양자얽힘 증명을 위한 Bell 테스트
 - (컴퓨팅분야) 양자계산우월성 증명을 위한 특수회로테스트



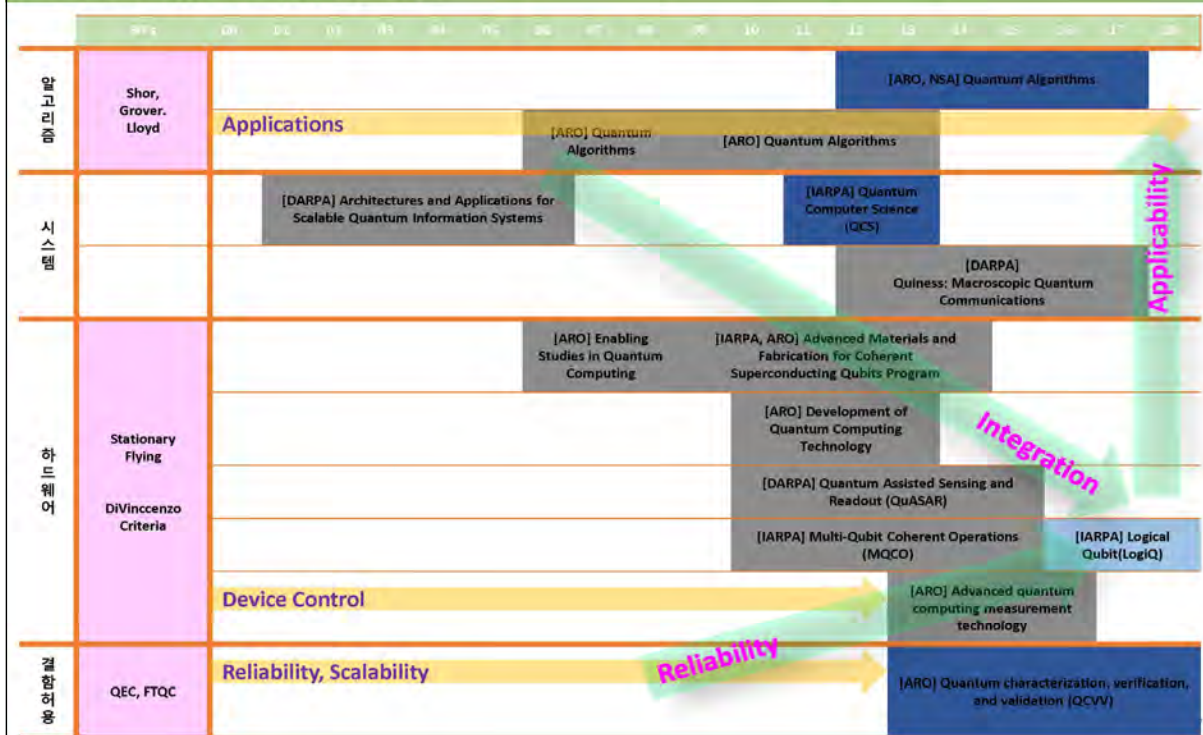
확보된 큐비트수와 큐비트유효시간에 따른 접근 영역

- 큐비트수, 유효시간에 따라서 활용방향성이 달라짐



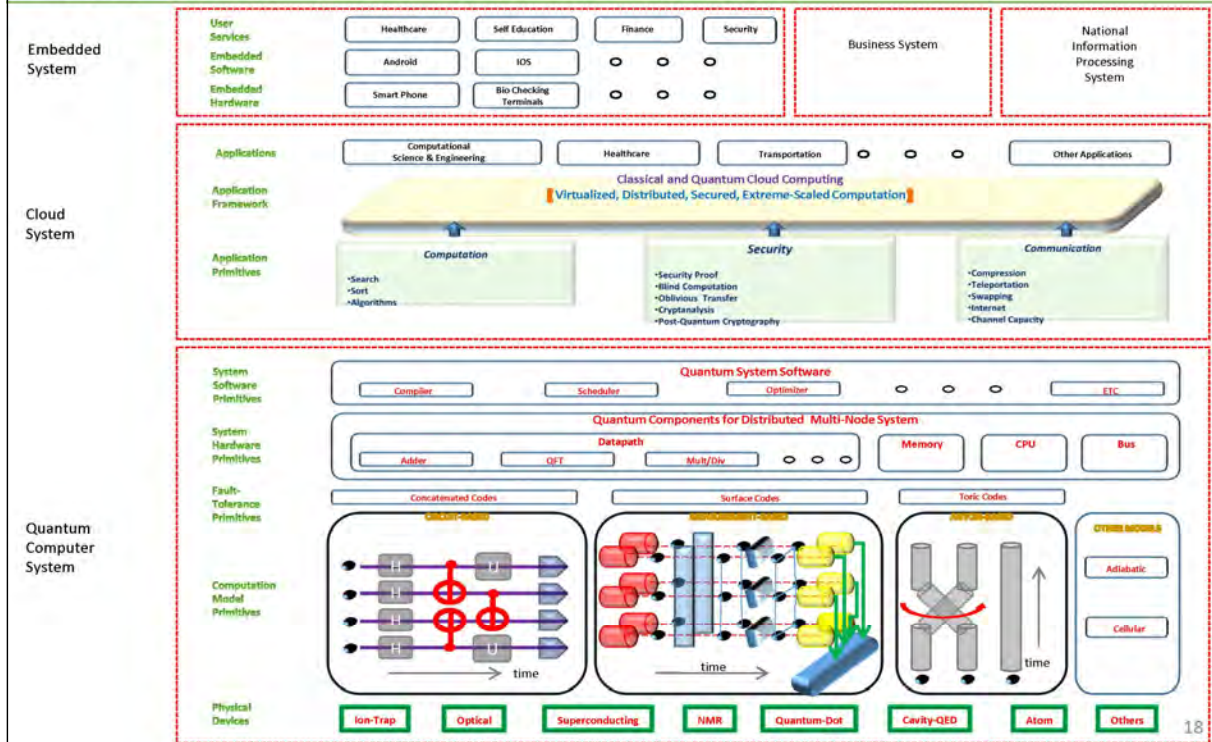
미국 정부/출연연 기준 양자컴퓨팅 연구개발 분석

- [구현단계를 넘어 실용화단계목적] 필요한 핵심역량의 강화를 목적으로 연구 프로그램들 진행
- [서비스단계]는 주로 기업군에서 진행



양자컴퓨팅 → 양자 ICT (양자클라우드형) 기본설계

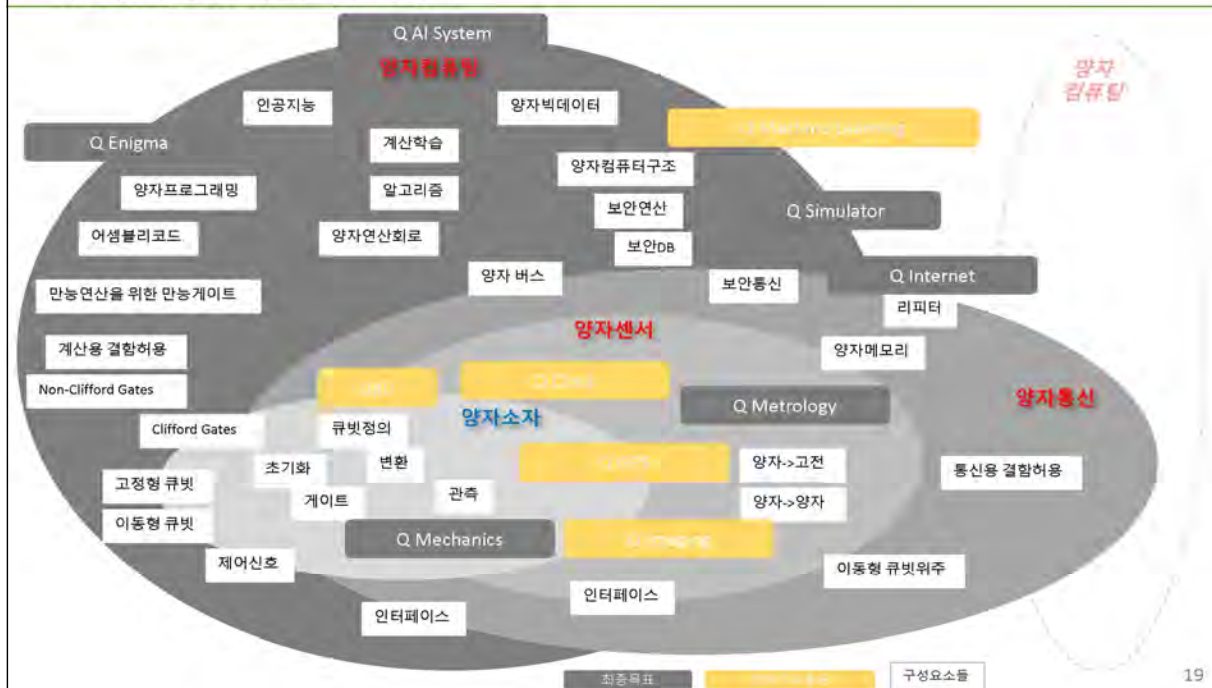
- 가장 하단부부터 가장 상단부까지의 기술적 상호 연계성
※ 기본적으로는 클라우드 형태에서 양자컴퓨팅 서비스가 제공될 예정



18

양자컴퓨팅과 다른 양자ICT영역과의 기술적 상관관계

- 양자역학, 양자소자 범위에서는 기초적인 실험, 개념/이론 증명
- 양자센서에서는 정보의 수집 및 표현
- 양자통신에서는 정보의 전달
- 양자컴퓨팅에서는 정보의 저장 및 처리



19

발제자 약력

성 명	김 태 현	
소 속	SK텔레콤 종합기술원 Quantum Tech. Lab	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
1991.03.~1995.02. 1995.03.~1997.02. 2000.09~2008.06.	서울대학교 서울대학교 Massachusetts Institute of Technology (MIT)	컴퓨터공학과 학사 제어계측공학과 석사 물리학과 박사
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
1997.08.~2000.06. 2008.06.~2011.08. 2011.09.~현재	공군사관학교 Duke대학교 SK텔레콤	전산통계학과 교관 및 전임강사 전기컴퓨터공학과 박사후과정 Quantum Tech. Lab Project Leader

세부발제 3 '양자암호통신 및 양자컴퓨터의 실용화/상용화 전망'

...

김 태 현
SK텔레콤 쿼텀테크랩

양자 암호 통신 및 양자컴퓨터의 실용화/상용화 전망

Taehyun Kim
Quantum Tech. Lab, Corporate R&D Center
SK telecom

III 주요국 정책 동향

정부 동향 요약

미국	<ul style="list-style-type: none"> • '09년 국가 양자정보 과학 비전 발표 • '16년 백악관 보고서 발표 • 산학연 연계 방식을 통해 4,766억원 투자 	영국	<ul style="list-style-type: none"> • '13년말에 향후 5년 동안 £270M를 투자 계획 발표
유럽	<ul style="list-style-type: none"> • '16년 양자정보통신 성명서 발표 • 향후 10년동안 €1B 투자 예정 	캐나다	<ul style="list-style-type: none"> • '10년 이전부터 정부 뿐만 아니라 민간기업에서도 양자 기술에 집중적으로 투자
중국	<ul style="list-style-type: none"> • 중장기 과학기술 개발 계획 ('05~'20)에 양자정보 연구 계획을 포함 • 13차 5개년 계획 ('16~'20)에 양자정보를 핵심 산업으로 지정하고 2,913억원 투자 	호주	<ul style="list-style-type: none"> • '11년부터 호주 연구위원회, 국방부, 뉴 사우스웨일즈 주 정부로부터 막대한 지원을 받아 CQC2T(Centre For Quantum Computation & Commun. Tech.)를 설립
일본	<ul style="list-style-type: none"> • '09년 FIRST프로그램을 통해 430억원 지원 • '40년까지 위성 양자 네트워크 구축 예정 	싱가폴	<ul style="list-style-type: none"> • '07년부터 정부주도로 1,300억원 이상의 예산 투자

III 목차

1. 양자암호 통신 현황

2. 양자 난수 발생기

3. 양자 컴퓨터 현황

4. Summary

양자 암호 주요 상용화 현황

양자 암호 통신 현황

미국	<ul style="list-style-type: none"> MagiQ: 초기 양자암호 장비 개발 및 IPR 다수 보유 Raytheon BBN: 최초 대도시내 양자 암호 시스템 설치/운영 Qubitekk: 양자 얽힘 광자 발생기 상용화 	일본	<ul style="list-style-type: none"> NICT: 도쿄 양자암호통신 네트워크 (JGN2 Plus) 구축 ('10년) NTT: 양자메모리가 없는 장거리 양자암호 전송 이론 개발
유럽	<ul style="list-style-type: none"> ID Quantique: 세계 최초 양자암호 통신시스템 상용화 Toshiba-Cambridge: 양자 암호 상용시스템 개발 KETS: 양자 암호 시스템용 광소자 개발 SeQureNet: 양자 암호 장비 개발 	중국	<ul style="list-style-type: none"> 안후이성-베이징 구간 양자암호시험통신망 구축 2,000km 구간(베이징-상하이) 양자 암호통신 백본망 건설중 양자암호통신 위성 발사 성공 Start-up: Quantum Ctek, Qasky 대기업: ZTE, Huawei
호주	<ul style="list-style-type: none"> Quintessence Labs: 양자 암호 시스템 및 양자 난수발생기 상용화 	한국	<ul style="list-style-type: none"> ETRI: 양자암호 송수신 시연 ('05년) SKT: 양자 암호통신 장비 상용화 및 시험망 구축 ('16년) KT-KIST: 양자통신 응용연구센터 개소 ('17년)

SKT 양자 암호 기술 개발 현황

양자 암호 통신 현황

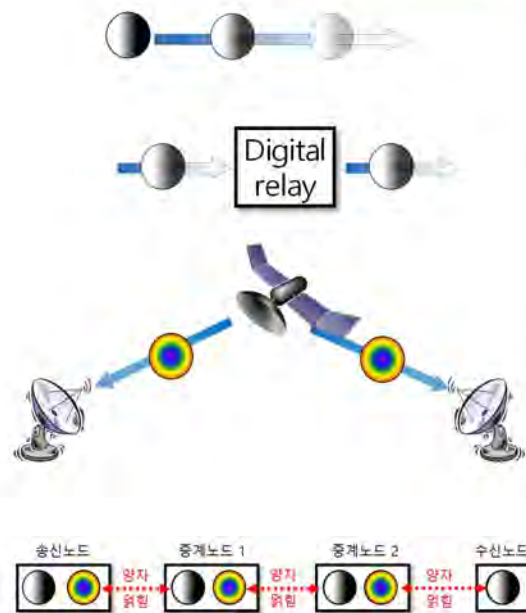
- 양자 암호 장비 개발
 - 암호키 발생 속도: 10 Kbps 이상 (50km구간)
 - BB84 + decoy 프로토콜
 - 암복호화 속도: 40 Gbps/slot
- 양자 암호 테스트베드 구축
 - 분당 지역과 대전(KISTI)에 양자 암호 테스트베드 구축
- Trusted repeater 개발
 - Trusted repeater를 이용해 총 112km 길이의 광섬유로 연결된 2개의 노드간의 양자암호 구현



양자 암호 장거리 적용

- 문제점: 광섬유내 광자의 흡수로 인해 광자의 장거리 전송에 한계가 존재함
- Trusted repeater
 - 현재 전세계 모든 양자암호 상용망에 적용하고 있는 방법
 - 중간에 양자 상태가 디지털로 변환되어야 하므로 보안성에 위험 존재
- 인공위성
 - 수직으로 대기층을 통과시 광자의 감소가 적다는 점을 이용
 - 얽힘 광자쌍 또는 단일 광자의 반사를 통해 양자 암호 구현
 - 전신과 같이 지상기지국의 지속적인 이동이 필요시 유리하나, 위성과 지상기지국간의 align 이나 기상 조건 등이 가장 큰 장벽임
- Quantum repeater
 - 양자 얽힘을 이용하여 중간에 디지털 변환없이 end-to-end로 양자 상태 유지
 - 광섬유 기반이므로 전신과 같이 지속적인 이동이 필요한 경우 한계가 존재함

양자 암호 통신 현황



5

중국 양자 암호 위성

Yin et al., *Science* **356**, 1140–1144 (2017) 16 June 2017

Satellite-based entanglement distribution over 1200 kilometers

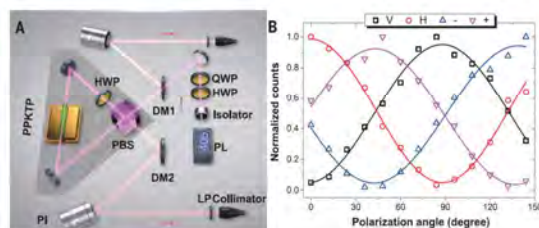


Fig. 1. Schematic of the spaceborne entangled-photon source and its in-orbit performance.

양자 암호 통신 현황

PHYSICAL REVIEW A **73**, 012316 (2006)

Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer

Taehyun Kim,^{*} Marco Fiorentino,[†] and Franco N. C. Wong

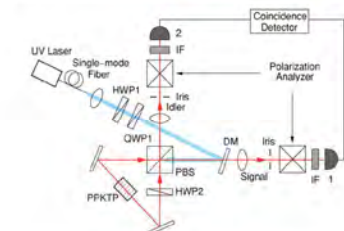
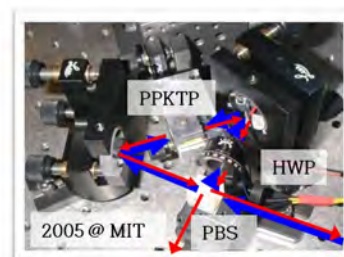


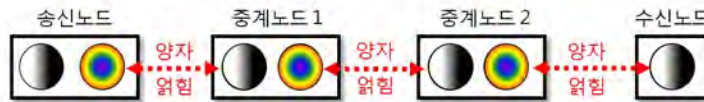
FIG. 2. (Color online) Experimental setup for polarization Sagnac.

6

SKT 양자 중계기 개발

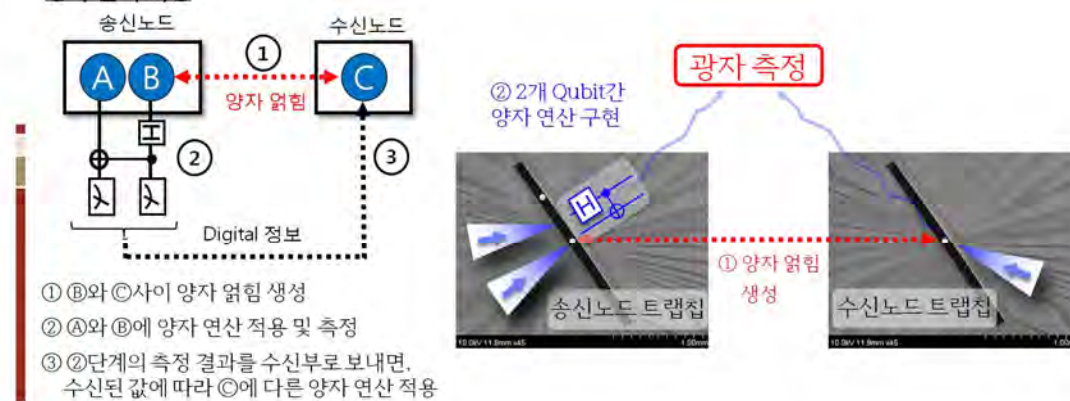
양자 암호 통신 현황

- 이온 트랩을 이용한 양자 중계기 개발



- 개발중인 기술: 양자 원격 이동에 필요한 핵심 요소 기술
 - 거리가 떨어진 2개 node간의 양자 얽힘(entanglement) 생성
 - 같은 노드 내의 2개 Qubit간의 양자 연산 구현

양자 원격 이동



7

목차

1. 양자암호 통신 현황

2. 양자 난수 발생기

3. 양자 컴퓨터 현황

4. Summary

양자 난수 발생기 상용화 현황

양자 난수 발생기

- 기술적인 배경
 - 대부분의 IoT 장치들이 암호화를 위해 난수를 사용함
 - 대부분의 현재 기술들은 알고리즘에 의해 발생된 유사 난수를 사용중임. 하지만, 유사 난수는 기본적으로 추측을 할 수 있는 가능성이 높음
 - 양자 중첩 상태의 측정 과정에서 발생하는 임의성은 측정이 일어나기 전까지 예측이 불가능하여, 진정한 난수 발생기로 사용 가능함.
 - 현재 많은 회사들이 양자 역학에 의한 난수 발생기를 상용화함.



[Quantis, IDQuantique]
- 4Mbps
- PCIe, USB
- photon dispersion



[PQRNG150, PicoQuant]
- 150Mbps
- USB
- photon arrival time



[qStream, Quintessence Lab]
- 1Gbps
- KMIP
- Fluctuation of vacuum states of light



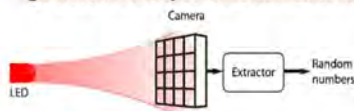
[Whitewood Entropy Engine, Whitewood Encryption Systems]
- 200Mbps
- PCIe
- bunching property of indistinguishable photons

SKT에서 개발중인 양자 난수 발생기

양자 난수 발생기

- SKT에서는 LED와 CMOS sensor로 이루어진 양자 난수 발생용 소형칩을 개발중임.

[Basic Principle of SKT QRNG]



PHYSICAL REVIEW X 4, 031056 (2014)

Quantum Random Number Generation on a Mobile Phone

Bruno Sanguinetti,^{*} Anthony Martin, Hugo Zbinden, and Nicolas Gisin
Group of Applied Physics, University of Geneva, Genève 4, CH-1211, Switzerland



• photon

- 칩크기: 5mm x 5mm



Aug. 2016

Nov. 2016

Jun. 2017

2Q 2018

End of 2018

Logic test +
ASIC design
Layout

FAB out +
Chip test

Engineering
sample

Commercialization

Certification from
Agencies

III 목차

1. 양자암호 통신 현황

2. 양자 난수 발생기

3. 양자 컴퓨터 현황

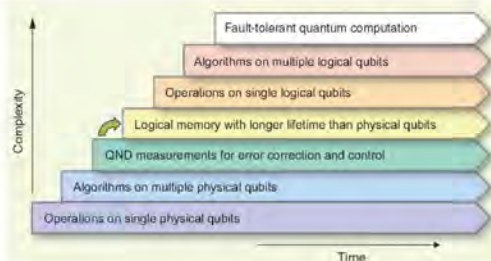
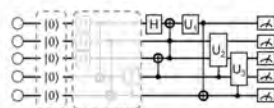
4. Summary

III 양자컴퓨터 관련 산업 동향

양자 컴퓨터 현황

	원자기반(중성 원자, 이온)	초전도체 기반	반도체기반(실리콘, 양자점, NV center 등)
양자 회로 기반 (양자 오류 정정 포함)	ionQ(이온) 	IBM  Google 	Intel-QuTech(양자점)  
Adiabatic		D-wave 	
위상학 큐비트		Microsoft-QuTech(초전도-나노와이어)  	

- 양자 회로 기반 양자컴퓨터 로드맵
 - Science 339, 1169 (2013)
 - 개별 양자 연산에서 발생하는 오류를 최소화하기 위한 Logical qubit 개발을 목표로 함



초전도체 큐비트

양자 컴퓨터 현황

IBM

- 2016년 5월에 5개 큐비트로 이루어진 양자컴퓨터를 클라우드 서비스 형태로 온라인에 공개함
- 2017년 5월에 16개 큐비트로 이루어진 양자컴퓨터를 공개함



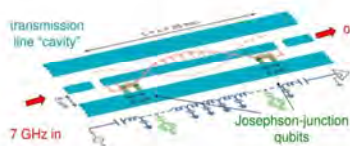
Google

- 현재까지는 9개 큐비트 양자프로세서 결과만 발표함
- 올해 양자컴퓨터를 클라우드 서비스로 공개할 예정임
- 올해말까지 약 50개의 큐비트로 이루어진 양자컴퓨터를 개발할 계획이라고 발표함

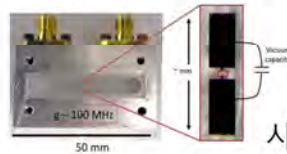


국내 현황

- 표준과학연구소에서는 3차원 transmon qubit 2개 이상을 이용한 실험을 진행중임



Transmon Qubit in 3D Cavity



사진출처: Yale대학 Qlab

13

이온 큐비트

양자 컴퓨터 현황

IonQ Inc.

- 이온 트랩 기반 미국 벤처 기업
- 초전도체에 비해 훨씬 더 긴 양자 결맞음 시간과 큐비트들간 임의의 연결이 가능함을 이용해 벤치마킹 결과를 발표. Proc. Natl. Acad. Sci. 114, 13 (2017)
- '16년에 22개의 이온 큐비트를 개별 제어 가능함을 보임
- '17년 최대 121개의 이온을 동시 포획 가능함을 보임
- '18년까지 32개의 이온 큐비트를 임의 제어 가능한 양자컴퓨터 개발 중

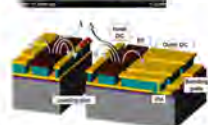
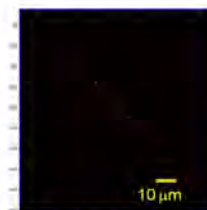
Table 2. Summary of the achieved success probabilities for the implemented circuits, in percentages

Connectivity	Star shaped			Fully connected		
	Superconducting			Ion trap		
Hardware	Obs	Rand	Sys	Obs	Rand	Sys
Success probability/%						
Margolus	74.1(7)	82	75	90.1(2)	91	81
Toffoli	52.6(8)	78	59	85.0(2)	89	78
Bernstein-Vazirani	72.8(5)	80	74	85.1(1)	90	77
Hidden shift	35.1(6)	75	52	77.1(2)	86	57



국내 현황

- 이온 포획용 칩 제작 기술 확보 및 이를 이용한 20개 이상의 이온 동시 포획 가능
- 1개 이온의 양자 상태 제어 가능
- 동일칩에 포획된 2개 이온 간의 연산을 위한 기술 개발 중임

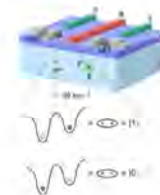
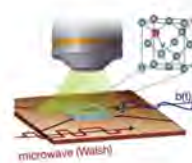
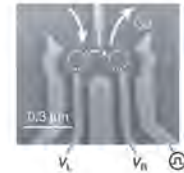


14

반도체 기반 큐비트

양자 컴퓨터 현황

- 반도체 기반 큐비트는 다음을 포함한 다양한 방법이 존재함
 - 양자점
 - 다이아몬드내 vacancy center
 - 핵스핀이 없는 기판내 불순물 원자
- 초전도체나 이온트랩에 비해 양자 상태 제어의 정확도는 낮지만, 향후 발전 가능성은 존재함
- 국내 현황
 - 최근 KIST, 서울대, ETRI 등 몇 개 기관에서 관련 연구를 진행중임

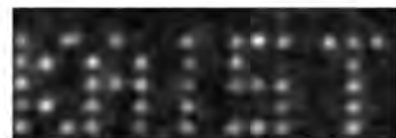
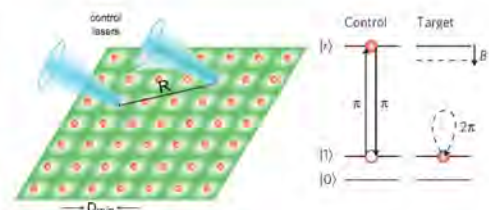


15

중성 원자 큐비트

양자 컴퓨터 현황

- 여러 개의 개별적인 중성원자들을 격자 또는 이와 유사한 형태로 포획 후, Rydberg 원자 상태를 이용하여 개별 원자의 양자 상태를 제어함
- 아직까지 상업화를 시작한 회사는 없음
- 국내 현황
 - 카이스트에서 40개 이상의 원자를 동시 포획 후 배열하는 기술 보유함
 - 1개 이상의 원자의 양자 상태 제어 기술 확보



16

Summary

- 많은 국가들이 최근 양자 정보 처리 분야에 대규모의 투자를 진행중임
- 양자 암호 시스템은 전세계 많은 회사들이 시스템 개발을 진행하였고, 점차 상용망에 적용이 시작됨
- 양자 난수발생기는 많은 회사들이 이미 상용 제품을 생산 중이고, SKT는 소형칩 형태의 양자 난수발생기를 생산할 예정임
- 양자 컴퓨터 분야에는 최근 전통적인 IT기업들이 많이 참여하여 향후 5년 내에 혁신적인 결과가 가장 많이 나올 것으로 기대되는 분야임

Ⅱ. 주발제

[R&D 및 산업화 전략]
‘양자기술의 국가 R&D 및 산업화 전략’

발제자 약력

성 명	문 성 욱	
소 속	한국과학기술연구원	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
1982.3~1986.2	연세대학교	금속공학 학사
1986.3~1988.2	연세대학교	금속공학 석사
1988.3~1994.8	연세대학교	반도체공학 박사
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
2015.1~현재	한국과학기술연구원	양자정보연구단장
2012.1~2014.12	한국과학기술연구원	나노양자정보연구센터장
2004.7~2012.1	한국과학기술연구원	나노시스템연구단장
2007.1~2008.1	한국과학기술연구원	나노바이오연구센터장
2004.10~2007.1	한국과학기술연구원	마이크로시스템연구센터장
2015.1~현재	한국과학기술연구원	차세대반도체연구소 책임
2002.3~2014.12	한국과학기술연구원	미래기술연구본부 책임
1997.2~2002.2	한국과학기술연구원	미래기술연구본부 선임
1995.6~1997.1	영국 Rutherford 연구소	우주연구부, 초빙연구원
1989.7~1995.6	한국과학기술연구원	광센서연구실 연구원

주발제 ‘양자기술의 국가 R&D 및 산업화 전략’

...

문 성 욱
한국과학기술연구원 양자정보연구단장

양자기술의 국가 R&D 및 산업화 전략

KIST 양자정보연구단

Contents

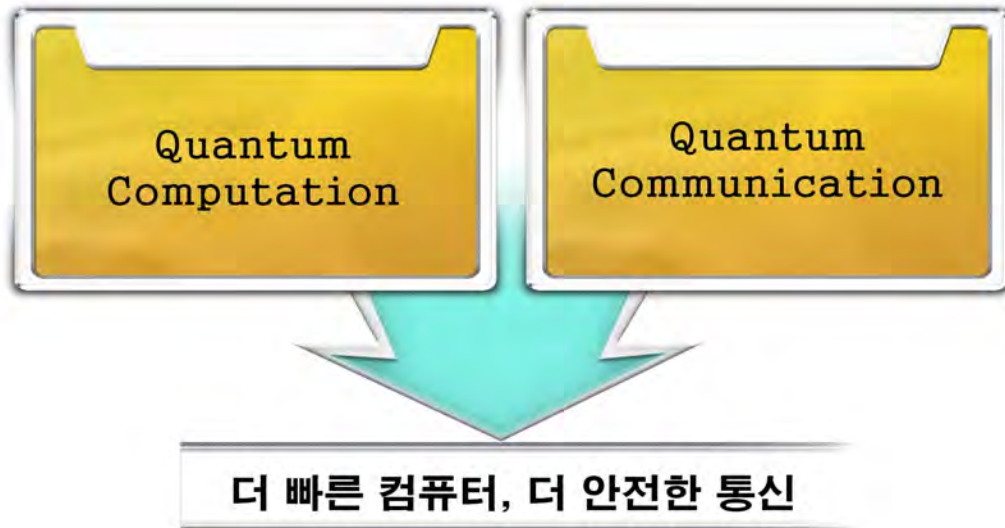
1. 양자기술의 분류
2. 양자컴퓨팅 기술의 국내외 기술수준 분석
양자컴퓨팅의 미래전망, 국가R&D 전략, 산업화 전략
3. 양자암호통신 기술의 국내외 기술수준 분석
양자암호통신의 미래전망, 국가R&D 전략, 산업화 전략
4. Summary

KIST Quantum Information Group

1. 양자기술의 분류

- ① Quantum Computing
- ② Quantum Communication
- ③ Quantum Metrology, Sensing & Imaging
- ④ Quantum Simulation
- ⑤ Quantum Information Theory

KIST Quantum Information Group



KIST Quantum Information Group

양자컴퓨팅

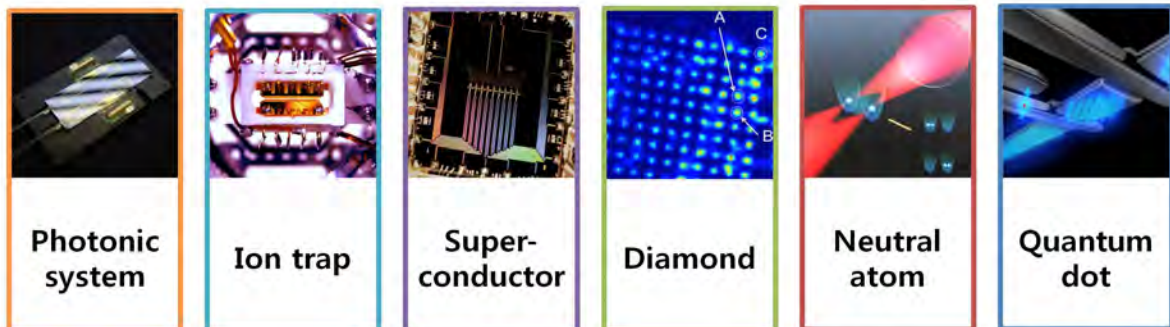
KIST Quantum Information Group

2.1. 양자컴퓨팅 기술의 발전단계

7	논리 qubit 및 양자오류 정정 코드 기반 Fault-tolerant universal 양자컴퓨팅 구현
6	양자오류 정정 기반 논리 qubit의 생성, 제어, 측정
5	다중 qubit 기반 양자우월성 (quantum supremacy) 검증 50여개 qubit의 전체적인 결맞음 유지하면서 양자연산
4	Small-scale 양자정보처리 프로세서 (Ion trap, Superconductor, Photon)
3	3개 이상 다중 qubit 양자 얽힘상태 생성 및 측정
2	2-qubit 얽힘상태 생성 및 측정 (2 큐비트 양자게이트 동작, CNOT)
1	단일 qubit 생성,제어,측정

KIST Quantum Information Group

2.2. 양자컴퓨팅 물리계의 종류

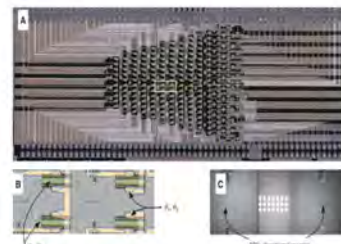
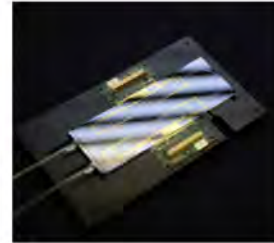


KIST Quantum Information Group

① Photonic system

세계 최고수준 (4단계)

- 영국 Bristol U. (4단계) ▶ Science 349, 711 (2015)
 - 5-qubit small-scale 양자정보프로세서 구현
- 중국 USTC (3단계) ▶ PRL 117, 210502 (2016)
 - 10-photon 양자얽힘 구현
- (진행중)
 - Boson sampling을 통한 quantum supremacy 구현 계획



국내 최고수준 (3단계)

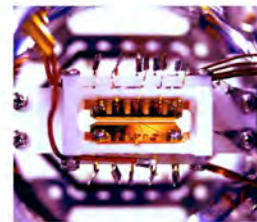
- POSTEC, KRISS (3단계)
 - 4 Photon 양자얽힘 및 측정 구현 (선형광학계 기반 2-qubit 양자게이트의 확률적 동작)

KIST Quantum Information Group

② Ion trap system

세계 최고수준 (4단계)

- 미국 UMD (4단계) ▶ Nature 536, 63 (2016)
 - 5-qubit small-scale 양자정보프로세서 구현
- 오스트리아 Innsbruck (3단계) ▶ PRL 106, 130506 (2011)
 - 14-qubit 양자얽힘 구현
- (진행중)
 - 50-qubit 양자얽힘 기반 quantum supremacy 구현 계획



국내 최고수준 (1~2단계)

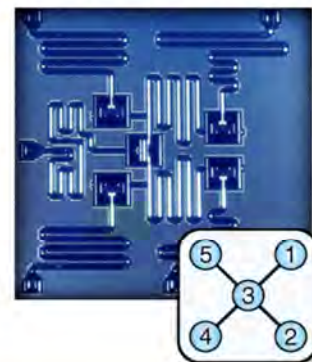
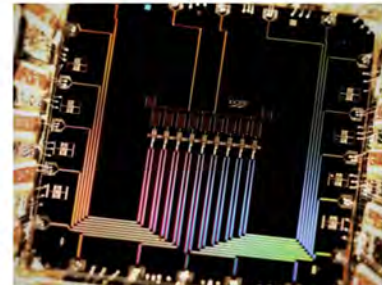
- SKT
 - 20개 qubit을 동시 포획 가능, 2-qubit 양자게이트 또는 양자얽힘 구현 중

KIST Quantum Information Group

③ Superconductor system

세계 최고수준 (4단계)

- 미국 UCSB (4단계) ▶ Nature 536, 441 (2016)
 - 5-qubit small-scale 양자정보프로세서 구현
- 3단계 (중국 USTC) ▶ arXiv : 1703.10302 (2017)
 - 10-qubit 양자얽힘 구현
- (진행중)
 - 50-qubit 양자얽힘 기반 quantum supremacy 구현 계획 (IBM)



국내 최고수준 (2단계)

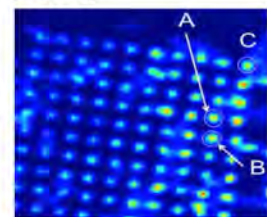
- KRISS (2단계)
 - 최근 2-qubit 양자게이트가 구현된 것으로 알려짐.

KIST Quantum Information Group

④ Diamond system

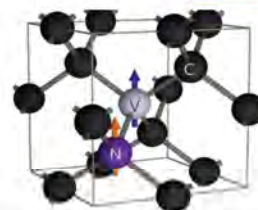
세계 최고수준 (3단계)

- 네덜란드 Delft U. (3단계) ▶ Nat. Nanotechnology 9, 171 (2014)
 - 3-qubit 양자얽힘 구현
- 독일 Stuttgart U. (2단계) ▶ Science 329, 542-544 (2010)
 - 2-qubit 양자게이트 구현
- (진행중)
 - Small-scale 양자정보프로세서 구현 중 (독일 Stuttgart U.)



국내 최고수준 (1~2단계)

- KIST (1~2단계)
 - 단일 qubit 생성, 제어, 측정. 다중 qubit 기반 양자노드 생성 및 2-qubit 양자게이트 구현 중.

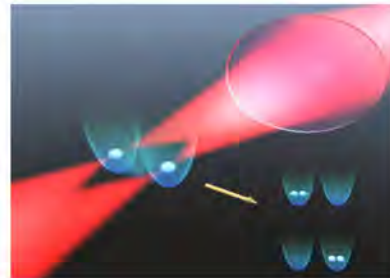
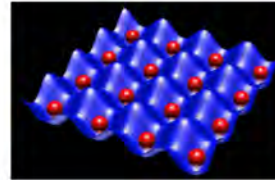


KIST Quantum Information Group

⑤ Neutral atom system

세계 최고수준 (3단계)

- 미국 Harvard (3단계) ▶ arXiv:1707.04344 (2017)
 - 51-atom array 이용, 양자 시뮬레이션 관측된 바 있음.
- 미국 JIRA (2단계) ▶ Nature 527, 208 (2015)
 - 2-qubit 양자게이트 구현
- (진행중)
 - Small-scale 양자정보프로세서 구현 계획
 - Atom array 기반 quantum supremacy 구현 계획



국내 최고수준 (3단계)

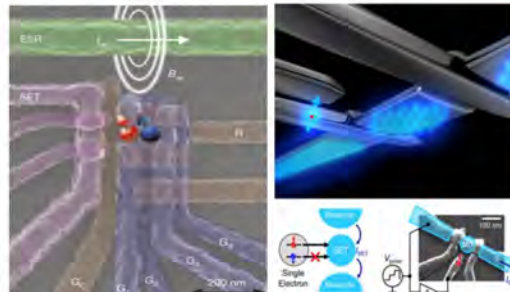
- KAIST (3단계)
 - 트위저 트랩을 이용하여 40개의 중성원자 포획 가능. 최근 19개의 qubit으로 Ising 모델 시뮬레이션. 다중 qubit 양자얽힘 생성 및 측정이 가능한 것으로 판단. (다중 qubit 확보가 용이한 장점이 있어 양자시뮬레이션에 특화된 연구가 주류, 2-qubit 양자게이트의 오류정정이 어려움)

KIST Quantum Information Group

⑥ Quantum dot system

세계 최고수준 (2단계)

- 호주 UNSW (2단계) ▶ Nature 526, 410 (2015)
 - 2-qubit 양자게이트 구현
- 스위스 ETH (1단계) ▶ Phys. Rev. Lett. 112, 116802
 - 단일 qubit 생성, 제어, 측정
- (진행중)
 - 3개 이상 다중 qubit 양자얽힘 구현

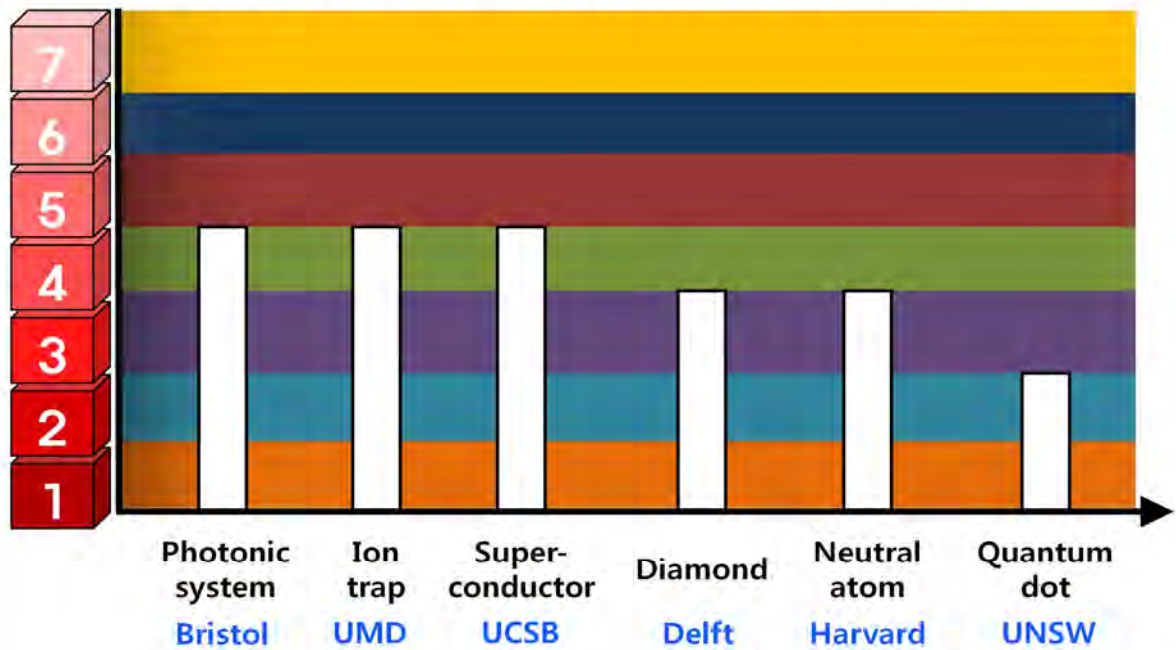


국내 최고수준 (1~2단계)

- SNU (1~2단계)
 - 단일 qubit 생성, 제어, 측정 가능. 다중 qubit 기반 양자노드 생성 및 2-qubit 양자게이트 시도 중.

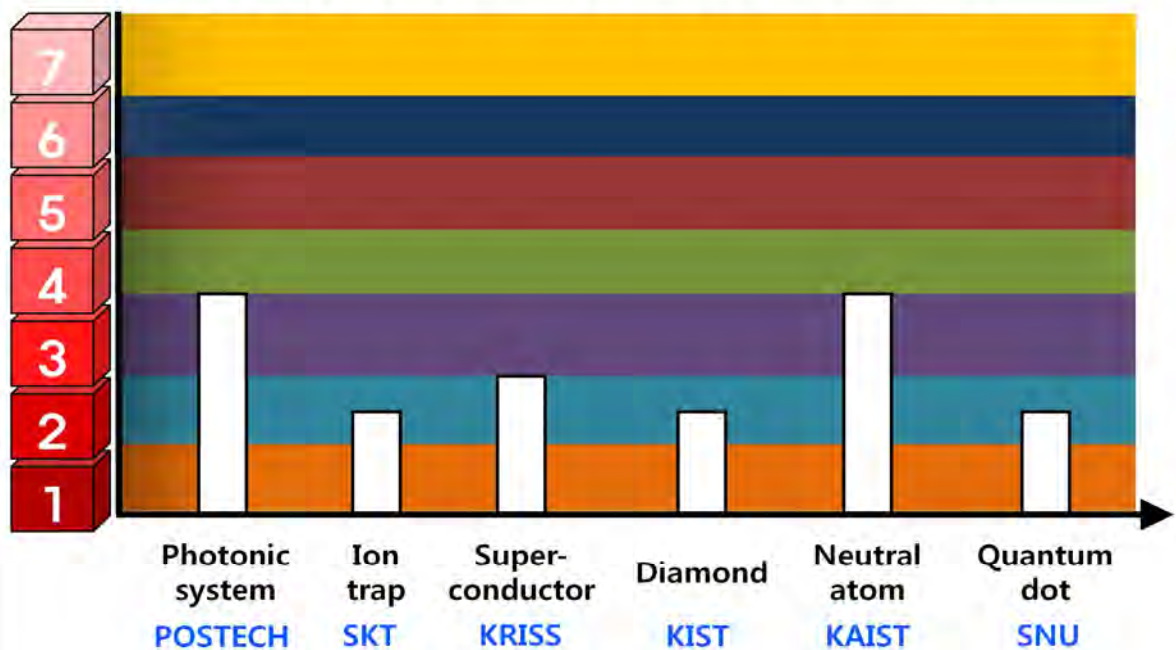
KIST Quantum Information Group

2.3 양자컴퓨팅 물리계 종류별 세계 기술 수준



KIST Quantum Information Group

2.4 양자컴퓨팅 물리계 종류별 국내 기술 수준



KIST Quantum Information Group

2.5 양자컴퓨팅 기술의 미래전망

- 1세대 컴퓨터 : 진공관 기반 (1940~1956) e.g. ENIAC
- 2세대 컴퓨터 : 트랜지스터 기반 (1956~1964) IBM 7090, 특수계산목적용
- 3세대 컴퓨터 : IC 기반 (1964~1971) e.g. IBM360, 초기 다목적 컴퓨터
- 4세대 컴퓨터 : VLSI 기반 (1971~현재) Personal, Super 컴퓨터
- 5세대 컴퓨터 : 양자컴퓨터가 될 것으로 예측

- 현재 수준은 디지털컴퓨터의 ENIAC에 해당됨.
- 디지털컴퓨터의 트랜지스터, IC, VLSI에 해당되는 기술도약이 어떤 물리계인지 불분명
- 2016, 영국 “양자기술을 위한 국가전략보고서”에 따르면, 가치 있는 어려운 문제를 해결할 large-scale 양자컴퓨터의 상업화 프로토타입은 10~20년 사이에 개발될 것으로 전망
- MIT 선정 10대 혁신기술 (2017.2.14)
- 세계경제포럼 선정 10대 미래유망기술 (2017.6.27)

KIST Quantum Information Group

2.6 양자컴퓨팅 기술의 국가 R&D 전략

- 양자컴퓨팅에 대한 연구는 아직 초기단계이므로, 어떤 물리계가 가장 유망한지에 대한 판단이 불가한 상태임. 현재는 특정 분야를 집중 투자하는 것을 논할 단계가 아님.
- Society의 건전한 발전을 위하여, 초기에는 다양한 분야를 동시에 지원하고, 점진적으로 소형 > 중형 > 대형과제로 집중 발전시키는 전략
- 철저한 Research base 연구지원을 통한 양자컴퓨터 연구에 대한 기초역량 확보 및 전문인력 양성



KIST Quantum Information Group

2.7 양자컴퓨팅 기술의 산업화 전략

- 산업화 수요는 특수계산 목적에 활용하기 위한 양자컴퓨터가 개발된 이후가 될 것으로 예상 (디저털컴퓨터의 2세대에 해당)
- 산업화로 연결시키기 위한 가장 시급한 문제는 Society 내부에 있는 연구자들의 협력체제 구축임 (공개적 검증, 과장된 낙관적 예측 배제)
- 공개적인 토론 및 검증을 유도하기 위한 “국가양자컴퓨팅 실무위원회” 신설 및 제한된 인력을 고려하여 선수가 심판이 될 수 있는 “통합평가단” 구성이 필요

KIST Quantum Information Group

양자암호통신

KIST Quantum Information Group

Introduction

Quantum Cryptography

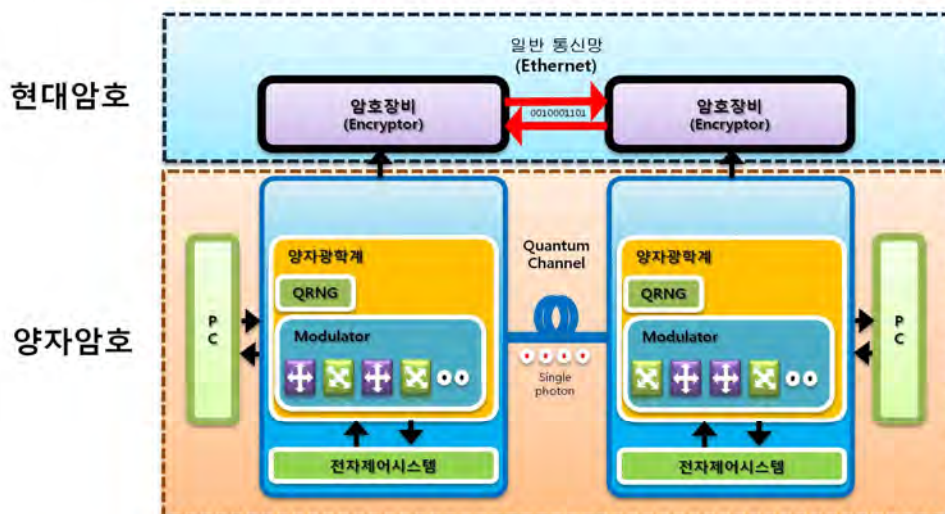
Flying qubits

Stationary qubits



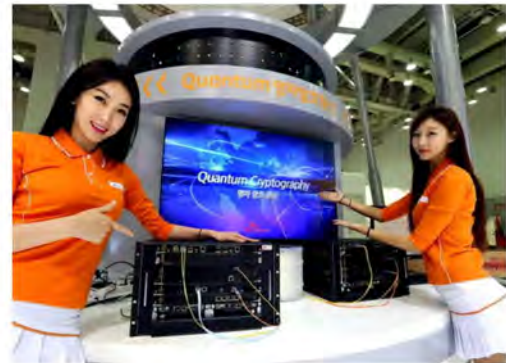
양자암호통신

양자가 갖는 복제불가능성을 이용해서, 멀리 떨어져 있는 송·수신자 (Alice와 Bob)가 통신상에서, 안전하게 비밀키를 나누어 가진 후, 이를 이용한 암호통신



양자암호통신 시스템 국내 구현 사례

- KIST 양자암호통신 system 개발
- Qcrypt'13 exhibition (2013)
- SKT 양자암호통신 시제품 개발
- WIS'14 exhibition (2014)



KIST Quantum Information Group

3.1 양자암호통신 기술의 발전단계

7	범용 개인용 기기 응용 (Consumer application)
6	Long distance quantum secure network (Quantum repeater, Satellite, Quantum signature)
5	1x1 특수목적용 상용화 서비스 (중국 신화통신, 유럽 스위스은행)
4	양자암호통신 테스트베드 실환경 검증 (한국, 일본, 캐나다, 미국, 중국, 스위스, 안정성 및 안전성 평가)
3	양자암호통신 장비 레벨의 시스템 개발 (Encryptor 연동, 현대암호와 결합된 양자암호통신)
2	양자암호키분배 장치의 연구실 규모 기본 성능 평가 (QBER, Quantum bit error rate 측정)
1	기초이론, 핵심기술 실험 검증 (양자암호프로토콜, 단일광자 생성 및 검출)

KIST Quantum Information Group

3.2 양자암호통신 기술의 미래전망

- **Post Quantum Computer** 시대를 대비하는 두가지 접근 방식인
수학적 계산복잡성에 기반한 PQC (Post Quantum Cryptography) 기술과
양자의 복제불가능성에 기반한 양자암호통신 (Quantum Cryptography)이
상호 경쟁보완적으로 발전
- 궁극의 보안솔루션은 양자암호통신을 통하여 구현될 전망

WHY

물리계층에서 도청을 원천적으로 방지할 수 있는
유일한 솔루션

KIST Quantum Information Group

3.3 양자암호통신 기술의 국가 R&D 전략

- **민간기업 연구와 차별되는 근본문제 해결형 연구**
 - **장거리 문제**를 해결하기 위한 인공위성, Quantum Repeater 연구 (장거리 문제해결을 위해 Trusted node를 사용하는 것은 임시방편적이므로 근본문제를 해결 해야 함)
 - **양자해킹 방지기술** 개발 (이론적으로는 완벽한 안전성을 보장하는 양자암호통신에서 부품들이 가지는 불완전성에 기인된 해킹 가능성이 보고 되고 있으며, 이를 방지할 수 있는 기술 개발이 필요)
 - **양자인증·양자서명** 기술 개발 (암호가 가져야 할 필요충분조건 중, 양자암호통신은 기밀성만을 보장하고 있고 나머지 조건은 현대암호에 의존하고 있으므로, 양자기술에 기반한 양자인증, 양자서명 기술이 개발 되어야만 모순을 해결할 수 있음)

KIST Quantum Information Group

3.4 양자암호통신 기술의 산업화 전략

- 대안기술인 PQC를 포함한 현대암호기술과 상호경쟁 보완협력
 - 암호포럼을 통한 공개토론회 개최
- 공개적인 검증시스템과 테스트베드 구축 및 표준화
 - 검증시스템을 국가망과 민간망으로 분리하고, 산업화 촉진을 위한 양자암호인증센터 신설
 - 접근 용이한 국가테스트베드 운영을 통한 기술 검증 기회 부여 및 산업생태계 활성화
- 공정한 기업참여 유도
 - 퀀텀조합 운영 주관 등을 단일 민간기업 주도에서 복수기업으로 전환
 - 공정한 산업체 경쟁 유도를 통한 기술 개발 촉진
- 국가기간망(행정망) 시범 적용을 통한 산업화 촉진



KIST Quantum Information Group

Summary

- 더 빠른 컴퓨터를 개발하고, 더 안전한 통신을 개발하는 것은 국가적 사명



KIST Quantum Information Group

Ⅲ

지정토론

토론좌장 약력

성 명	이 석 한	
소 속	한림원 학술담당부원장(성균관대학교)	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
1972	서울대학교	학사
1974	서울대학교	석사
1982	Purdue University	박사
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
1974~1978	육군사관학교 인하대학교	교수요원 전임강사
1983~1997	USC (남가주 대)	조교수, 부교수(겸직), 정교수(겸직)
1990~1997	NASA JPL/Caltech 지능로봇연구	Leader/책임연구원
1995	KAIST	초빙교수
1998~2003	삼성종합기술원	전무, 연구소장, Chief Research
1998~현재	USC (남가주 대)	Officer
2002	National Technology Roadmap (NTRM) 사업단	겸임교수
2002~현재	21세기 프론티어사업 나노메카트로닉스 운영위원회	단장
2003~현재	성균관대 정보통신공학부 지능시스템연구소	위원장 정교수
2003	과학기술부 차세대 성장 동력 기획단	소장(겸)
2004~현재	Intelligent Service Robotics J. Springer	단장
2004~현재	IEEE Robotics and Automation Society	Editor-in-Chief
2004~현재	한국 로봇공학회	부회장
2005~현재	IEEE Sensors Conference 2006	부회장
2005~현재	한국 지능 로봇 표준화 Forum	General Chair
2010~현재	우주로봇협의회	의장
2011~2012	성균관대학교	회장 대학원장

토론자 약력

성 명	김 길 호	
소 속	성균관대학교 전자전기공학부	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
1981. 03.~1985. 02.	한양대학교	물리학 학사
1990. 03.~1992. 08.	한양대학교	물리교육학 석사
1993. 10.~1998. 07.	University of Cambridge	물리학 박사
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
1999.02~2002.02 2002.03~현재	한국전자통신연구원 (ETRI) 성균관대학교	선임연구원 교수

토론요약문

김 길 호

성균관대학교 교수

양자 컴퓨터 (Quantum Computer)

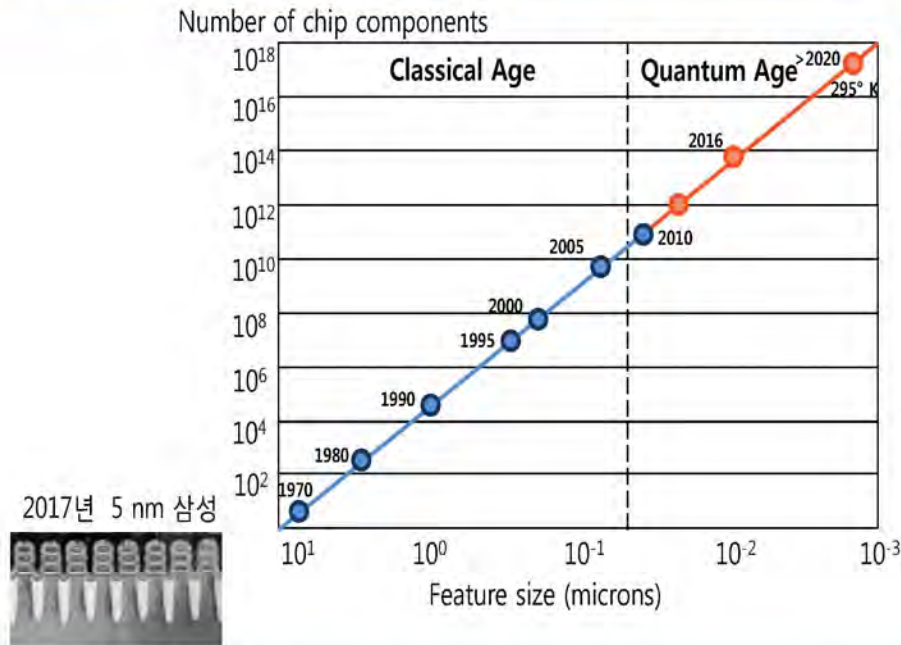
김 길 호

성균관대학교 전자전기공학부

2017년 8월 18일 한림원



Leap-frog to atomic-scale device fabrication



Sungkyunkwan University (SKKU)

Semiconductor Nano Device Lab.

실용적인 양자 컴퓨팅 응용

Optimization	Machine learning on Big Data	Quantum Simulation	Prime Number Factorization
<p>Applications Include:</p> <ul style="list-style-type: none"> Investment allocation and portfolio management Workforce allocation and scheduling Optimization distribution systems, especially fleet routing (최적화 분배 시스템, 특히 신속 라루팅) Manufacturing process optimization Working capital and cash management Inventory planning 	<p>Applications Include:</p> <ul style="list-style-type: none"> Search engine optimization (검색 엔진 최적화) Error detection in engineering data Genetic/biological research Statistical physics & chemistry Weather forecasting and climate modeling Risk & financial modeling Object, facial speech recognition Medical diagnosis Fraud detection 	<p>Applications Include:</p> <ul style="list-style-type: none"> Quantum physics including fluid dynamics and chemistry research Rapid verification and validation for engineering problems Simulations of protein folding and other advanced biochemical processes Quantum chemistry of new and exotic materials (새롭고 이국적인 물질의 양자 화학) 	<p>Applications Include:</p> <ul style="list-style-type: none"> Decryption and code breaking (암호 해독 및 코드 분할) Breaking evolved natural codes in bioinformatics Mathematical research

50 different quantum algorithm registered <http://math.nist.gov/quantum/zoo/>



Sungkyunkwan University (SKKU)

Semiconductor Nano Device Lab.

Overview: Different types of qubits

TABLE I. Comparison between different systems used as qubits.

	Atom, molecule, ion	Electron spin	Nuclear spin	Superconducting qubit
Size	$\sim 10^{-10}$ m	$\sim 10^{-10}$ m (impurities) $\sim 10^{-8}$ m (quantum dot) ^a	$< 10^{-10}$ m ^a	$\sim 10^{-6}$ m
Energy gap	10^5 – 10^6 GHz, \sim GHz (Rydberg atoms)	1–10 GHz	1–10 MHz	1–20 GHz
Frequency range	Optical, microwave	Microwave	Microwave	Microwave
Operating temperature	nK to μ K	~ 100 mK (quantum dot), room temperature (NV center)	\sim mK	~ 10 mK
Single-qubit gate operation time τ_1	$\sim \mu$ s (atom) ~ 50 ps (ion)	~ 10 ns	> 10 μ s	~ 1 ns
Two-qubit gate operation time τ_2	$\sim \mu$ s (atom) ~ 100 μ s (ion)	~ 0.2 ns	~ 10 ms	~ 10 – 50 ns
Coherence time T_2	ms to s	ms to s	\sim s	~ 10 – 100 μ s
T_2/τ_1	10 – 10^4	10^5 – 10^8	10^6	10^4 – 10^5
Coupling type	Electric or magnetic	Magnetic or electric	Magnetic	Electric or magnetic
Coupling strength with the cavity	$< \text{kHz}$ (B field), ~ 10 kHz (E field), ~ 10 MHz (Rydberg atoms)	$> \text{MHz}$ (quantum dot) ~ 100 Hz (impurities)	~ 0.1 Hz	~ 0.1 – 1 GHz

Z.L. Xiang Rev. Mod. Phys 85,623 (2013)

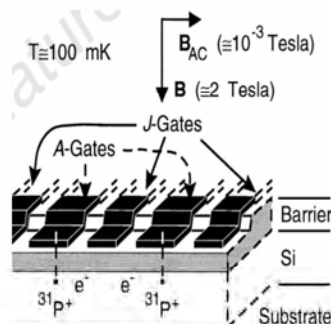


Sungkyunkwan University (SKKU)

Semiconductor Nano Device Lab.

Donor based silicon quantum computer

Qubit are the nuclear spin of ^{31}P donor atoms in ^{28}Si



B.E. Kane, Nature 393, 133 (1998)

Advantages:

- Relaxation T long (> 10 hours)
- Low spin-orbit coupling
- Spin free host existing multi-billion dollar silicon microelectronics industry

Disadvantages:

- Require the ability to dope Si with atomic precision aligned to nanometer sized surface gates

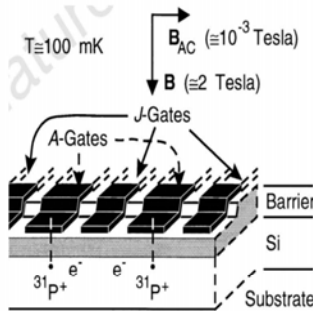


Sungkyunkwan University (SKKU)

Semiconductor Nano Device Lab.

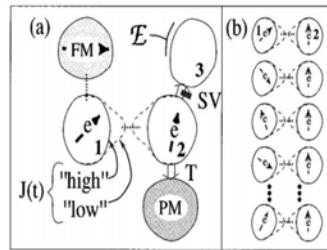
Theoretical proposal for qubits in silicon

Nuclear spins of P donors



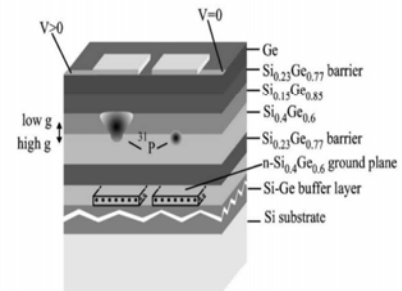
B.E. Kane, Nature 393, 133 (1998)
A.J. Skinner, Phys. Rev. Lett. 90, 087901 (2003)

Electron spins in quantum dots



D. Loss and D. P. DiVincenzo
Phys. Rev. A 57, 120 (1998)

Electron spins of P donors



R. Vrijen et al.
Phys. Rev. A 62 012306 (2000)

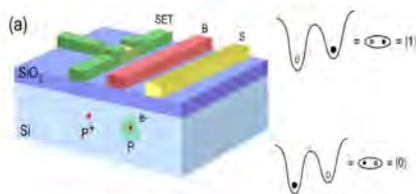


Sungkyunkwan University (SKKU)

Semiconductor Nano Device Lab.

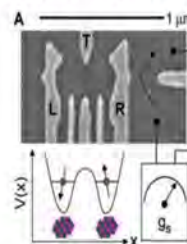
Theoretical proposal for qubits in silicon

P donor charge qubits



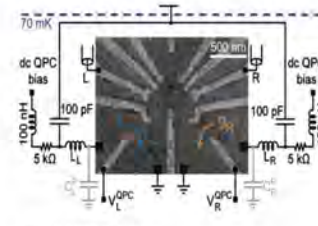
L.C.L. Hollenberg et al,
Phys. Rev. B 69, 113301 (2004)

Singlet-triplet qubit



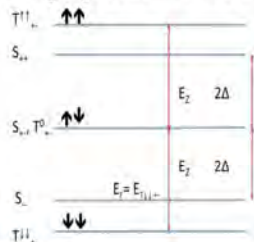
J.R. Petta et al. Science 309, 2180 (2005)
Q. Li et al. Phys. Rev. B 81, 085313 (2010)

Exchange only qubit



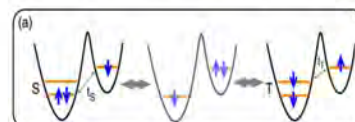
E. Laird et al,
Phys. Rev. B 82, 075403 (2010)

Valley qubits in silicon



D. Culcer et al,
Phys. Rev. Lett. 108,
126804 (2012)

3 electron quantum dot hybrid qubit

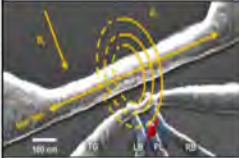


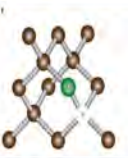



Z. Shi et al.
Phys. Rev. Lett. 108 140503 (2012)



Sungkyunkwan University (SKKU)

Semiconductor Nano Device Lab.

Silicon spin qubits	Superconducting loops	Ion traps	Diamond vacancies	Topological qubits
				
Longevity: 30 secs Logic success rate: 99.9 % Number entangled: 2	Longevity: 0.00005 secs Logic success rate: 99.4 % Number entangled: 17	Longevity: 1000 secs Logic success rate: 99.9 % Number entangled: 14	Longevity: 2 secs Logic success rate: 99.2 % Number entangled: 2	Longevity: untested Logic success rate: ? Number entangled: ?
Pros: Spin free environment, high stability, record longevity in solid state, reproducibility, manufacturability	Pros: Flexibility, fast, ongoing improvements in longevity, easy to fabricate	Pros: One of the first designs, very stable, on-chip designs underway.	Pros: Interact with light, room temperature operation	Pros: topological protection from errors, reduced qubit density for error correction
Cons: Interconnects challenging: only a few entangled	Cons: stability, space requirement, low temperatures required	Cons: requires ultra-high vacuum, many lasers, slow operation	Cons: Difficult to fabricate, reproducibly with precision placement and difficult to entangle	Cons: no qubit demonstrated, low temperatures and highly controlled electromagnetic environment
Companies: Intel, HRL	Companies: DWave, IBM, Google, Rigetti, Quantum Circuits, Intel	Companies: IonQ	Companies: Quantum Diamond Technologies	Companies: Microsoft, Bell labs
Research leaders: UNSW, Wisconsin, Sandia, UCL, Princeton, Riken, TUDelft	Research leaders: UCSB, Berkeley, Yale, Zurich, TUDelft, MIT	Research leaders: Innsbruck, NIST, Oxford, Maryland, Sussex, MIT	Research leaders: TUDelft, Stuttgart, Harvard, Chicago	Research leaders: TUDelft, Niels Bohr, Maryland, UCSB

토론자 약력

성명	김 용 주	
소속	전자신문 통신방송부	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
2010~2017	전자신문사	통신방송부 기자

토론요약문

김 용 주

전자신문 통신방송부 기자

양자정보통신, 과감한 정부 투자 필요한 때

양자정보통신(Quantum ICT)으로의 이행은 자명해지고 있다. 프로펠러 시대에 제트 엔진의 발명을 지켜본 사람이 공중전 패러다임의 변화를 예측하는 것과 같이, 양자정보통신의 태동을 지켜본 사람이라면 누구나 ‘지금까지와는 전혀 다른 정보통신기술(ICT) 시대가 열릴 것’임을 직감할 수 있다.

양자정보통신에 국가적 투자가 이뤄지지 못해 안타깝다. 과학 강국은 정부가 나서 투자를 독려하는데 한국은 민간 기업이 소규모 투자를 하는 수준에 머무르고 있다.

정부 투자가 더딘 가장 큰 원인은 ‘경제성(비용 대비 효율)’을 따지기 때문이다. 세금을 투자하면 얼마의 이익이 남느냐는 ‘계산서’가 필요하다는 것이다. 하지만 시장이 열리지 않은 분야에서 정확한 경제성 계산은 무의미하다. 시장이 형성된 뒤 투자하는 것은 이미 늦다. ‘우리가 시장을 만든다’는 생각의 전환이 필요하다. 당장은 경제성을 계산하기 곤란하지만, 수년 안에 시장이 열릴 것으로 보이는 기술에 과감한 투자가 필요하다.

‘경제성이 떨어지는 상용 기술 대신 양자 기초 기술에 투자해야 한다’는 목소리가 나오는 것은 우려스럽다.

우선 ‘내부 갈등’으로 비칠 수 있다. 기초 기술과 상용 기술은 한 몸이다. 협력 대상이지 배척 대상이 아니다. 서로 협력할 때 최상의 결과를 얻는다.

양자 기술 상용화가 가시화한 시점에 국책과제로 기초 기술에 투자하는 것은 설득력이 떨어진다. 세계 각국이 상용화 경쟁을 시작했다. 경쟁에 뒤처지지 않기 위해선 국책과제 자금을 상용 기술 개발에 집중해야 한다. 지금 필요한 건 단거리 육상선수이지 마라톤 선수가 아니다.

기초 기술 개발을 소홀히 하는 것은 물론 안 된다. 국책과제가 아니라 다른 연구개발(R&D) 비용을 투자하는 방안이 좋은 대안으로 보인다.

토론자 약력

성 명	박 성 수	
소 속	한국전자통신연구원 미래전략연구소 기술기획연구그룹	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
1986.3.~1992.2.	KAIST	재료공학 (박사)
1984.3.~1986.2.	KAIST	재료공학 (석사)
1980.3.~1984.2.	연세대학교	금속공학 (학사)
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
2016.3.~현재	TTA	전략계획위원회 부의장
2006.11.~2007.10.	UC Irvine	전기전자컴공과 초빙연구원
2004.9.~2008.2.	과학기술연합대학원 대학교	컴퓨터공학과 부교수/교수

토론요약문

박 성 수

한국전자통신연구원 미래연구부장



양자정보통신 관련 기업의 투자현황 1/2

연도	기업체	투자금액	비고
1999~2016	D-Wave	USD 1.4억	초전도 기반 양자어닐링 머신 개발 사로 주요 투자자는 Harris & Harris Group, Draper Fisher Jurvetson, Goldman Sachs, In-Q-Tel(미국 CIA), Bezos Expeditions(아마존 설립자)
2006~현재	Microsoft	미상	양자컴퓨터용 범용 프로그래머, SW를 개발 중으로 수백만달러 투자 예상
2009~현재	Google	미상	자체개발 및 NASA와의 D-Wave시스템 공동 구매하여 인공지능, 탐색엔진으로 사용
2011~현재	Lockheed Martin	미상	D-Wave 최초 구매자로 항공기 설계에 활용
2012	Raytheon BBN	USD 220만	광자소자 기술에 대해 IARPA로부터 지원 받음
2013	Quantum Valley Investments	USD 1억	Blackberry 설립자 지원의 양자컴퓨팅 펀드
2014	IBM	USD 30억	초전도 양자컴퓨팅을 포함한 5년간 나노기술 투자
2014	Rigetti Computing	USD 300만	D-Wave SW 회사로 Y Combinator가 주요 투자자
2014	Qubitekk	USD 300만	광자소자개발로 미국 에너지성 과제 수주
2015	1QBit	미상	D-Wave 응용SW회사로 주요투자자는 CME Group (Series A) 및 RBS Solutions
2015	Alibaba Group	CNY 1.5억	2015년부터 5년간 양자컴퓨팅 응용 연구
2015	Cambridge Quantum Computing Ltd	USD 0.5억	D-Wave용 SW개발사로 Grupo Arcano가 3년 이상 투자함

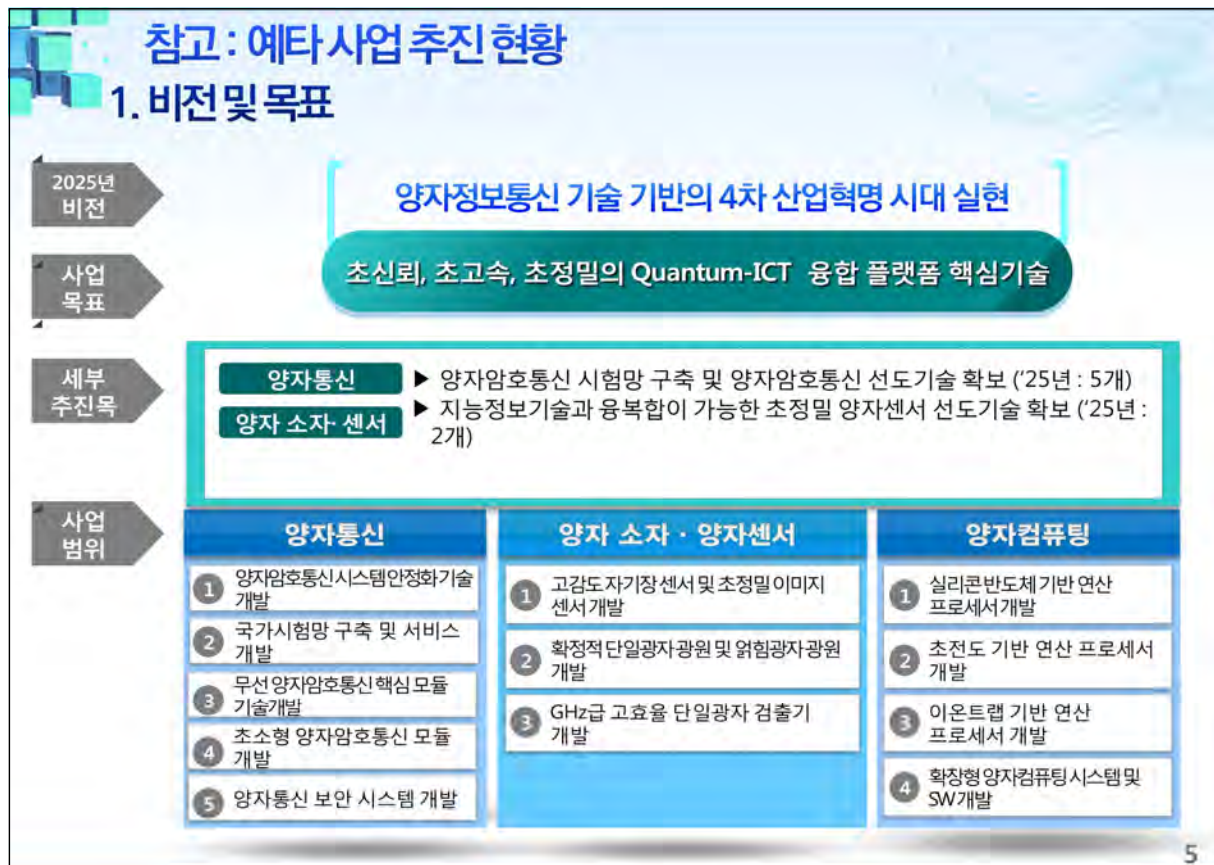
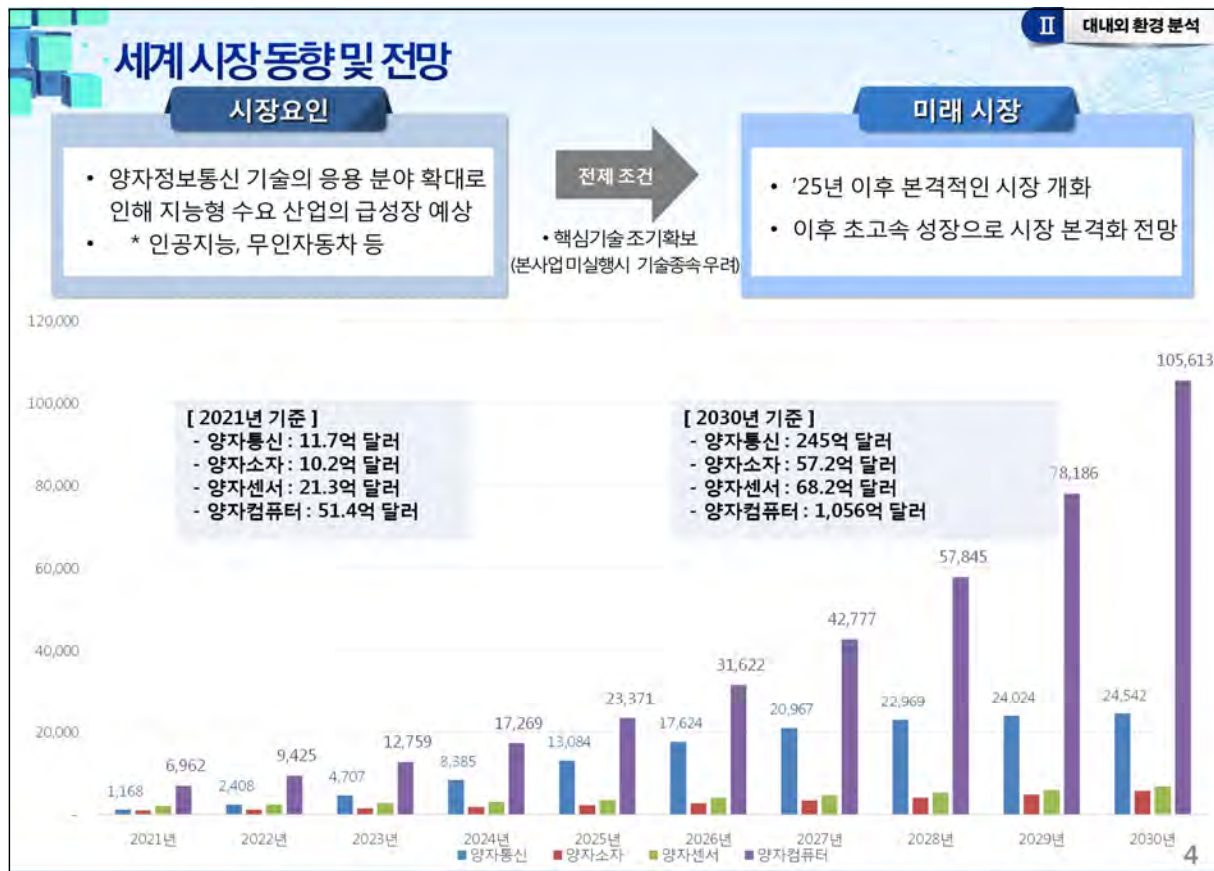
출처 : <https://www.cbinsights.com> 및 Oxford, "The Commercial Prospects for Quantum Computing", 2016, 12.

2

양자정보통신 관련 기업의 투자현황 2/2

연도	기업체	투자금액	비고
2015	Commonwealth Bank of Australia (CBA)	AUD 1500만	반도체기반 양자컴퓨팅 관련 투자
2015	IBM	미상	IARPA프로그램으로 초전도기반 범용양자컴퓨터 과제 수행
2015	Intel	USD 0.5억	Delft 대학, TNO(네덜란드응용기술개발기구)에 투자하여 반도체기반 및 초전도 큐비트 개발
2015	Playground Global	USD 3억	안드로이드 창시자인 Andy Rubin, Peter Barrett, Matt Hershenson and Bruce Leak이 만든 벤처펀드
2015	Telstra	AUD 1000만	반도체기반 양자컴퓨팅 연구에 투자
2016	Alibaba Group	USD 10억	양자클라우드컴퓨팅을 위해 Nvidia와 전략적 협정
2016	Quantum Circuits, Inc	-	양자컴퓨팅 SW기업으로 펀드모집 중
2016	TundraSystems Global Ltd	-	광자기반 양자컴퓨터로 펀드모집 중
2017	Rigetti	USD 0.64억	초전도양자컴퓨터 Y Combinator's Continuity 등
2017	IonQ	USD 0.22억	이온트랩양자컴퓨터, NEA 및 GV(Google Venture)로부터 펀딩

3



발제자 약력

성 명	백 정 현	
소 속	(주)이와이엘	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
1995~1997 1989~1995	아주대학교 대학원 아주대학교	공업화학과 석사 공업화학과 학사
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
2015~현재 2013~2014 2011~2014 2003~2011 2000~2003 1996~2000	(주)이와이엘 하이밸류컨설팅 프론티어솔루션 BearingPoint (구KPMG컨설팅) 아더앤더슨 LG CNS	기획본부장, 상무 상무 PI 사업부장, 상무 이사 부장 대리

토론요약문

백 정 현
(주)EYL 상무

양자산업을 위한 스타트업 육성

(주)이와이엘 백정현



1. 회사 개요



회사명:	(주)이와이엘
대표이사:	정부석
홈페이지:	www.eylpartners.com
직원 수:	9명
창업일:	2015년 1월 8일
법인위치:	(본사) 경기도 용인시 기흥구 영덕동 (연구소) 경기도 성남시 분당구 이매동
해외법인:	미국 법인 - Washington D.C. 일본 연락사무소 - Tokyo
사업내용:	Micro QRNG(Quantum Random Number Generator, 초소형 양자난수 생성기) 핵심기술 및 응용제품

2. 기술 소개 - 원천기술 확보

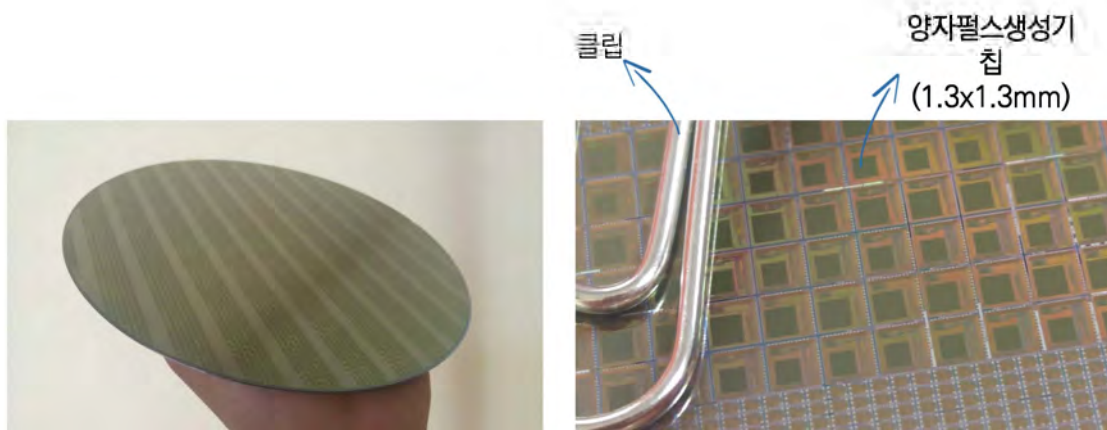
- 난수생성기는 보안에서 가장 중요한 암호키를 제공
- 대부분의 난수생성기는 수학적 프로그램으로 만들어(유사난수생성기) **해킹 위험**
- 자연현상에서 발생하는 노이즈를 이용한 난수생성기(진정난수생성기)는 안전하지만 **크고 비싸고 비효율적**, 고전물리학 결정론에 근거하여 예측 가능, **보안 시스템에 부적합**
- 예측 불가능하고 가장 신뢰성이 있어서 보안 시스템에 적합한 양자난수생성기가 가장 좋지만 **상용화된 양자난수생성기는 크고(server 사이즈), 비싸고(수천만 원), 비효율적(편향성 보정을 위한 많은 부품 탑재)**
- 이와이엘은 세계 최초로 방사성 동위원소의 자연붕괴 현상을 이용한 **"초소형 양자난수 생성기와 응용솔루션"**을 칩으로 개발하여 IoT 보안에 폭넓게 적용 될 수 있는 **"원천 핵심 기술"**을 보유



이와이엘의 초소형 양자펄스생성기
(5mm x 5mm)

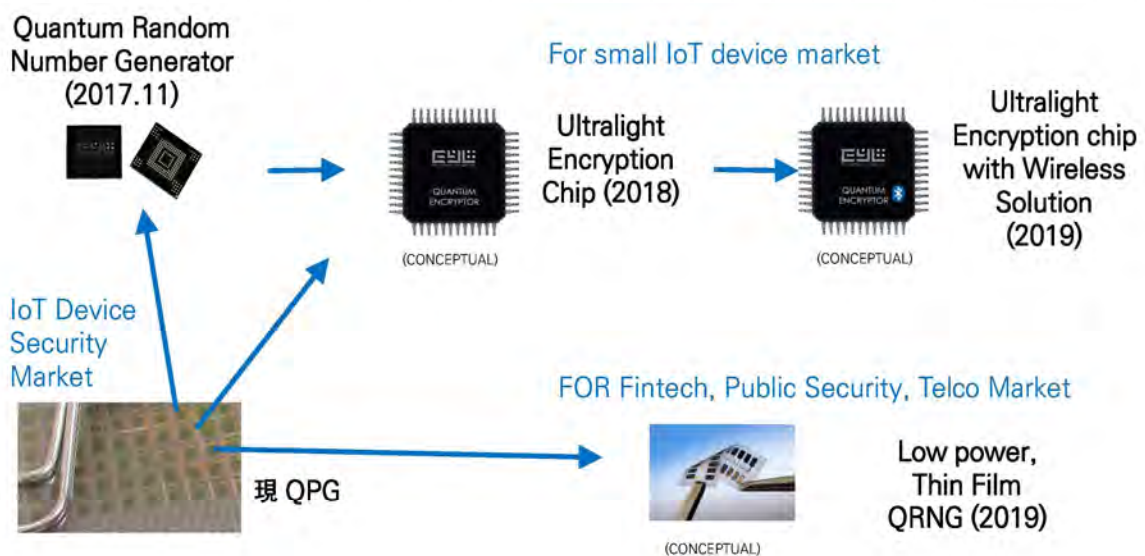
2. 기술 소개 - 상용화 시작

기존 5mm 크기의 QPG를 1.3mm 크기의 wafer로 개발에 성공, 향후 더 작은 양자난수생성 칩 및 초경량 암호 칩으로 상용화 시작



2. 기술 소개 - 향후 방향

개발 완료 된 QPG는 초경량 암호 칩과 필름형 양자난수생성기로 발전



2. 기술 소개 - 응용시스템

현재 USB 또는 PCI Express형태로 초소형/초고속 양자난수생성기를 개발하여 상용화 하였으며 관련 응용 시스템 출시 중



세계최초 방사성동위원소를 이용한
초소형/초고속 양자난수생성기



양자난수생성 기술을 활용한
정보자산 관리용 USB 저장장치

3. 해외 진출 - 매스챌린지

2016년 세계 벤처 올림픽 “매스챌린지” 보스턴 대회에서 5,500개 스타트업을 제치고 우승

“THE MOST SHINING STARTUP ON THE PLANET”
- John Harthorne (매스챌린지 CEO) -

23 개국,
5,500 스타트업 참가,
128 결승 진출팀 선발,
4 개월간 보스턴 현지에서 경쟁

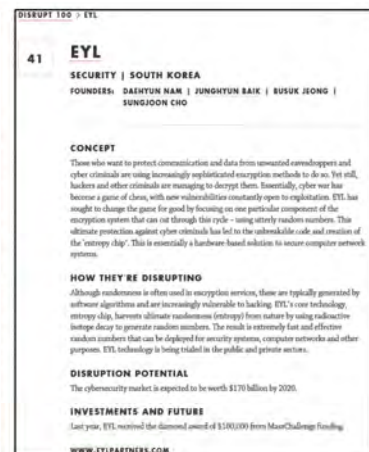
MC
MASSCHALLENGE

2016 DIAMOND WINNER

3. 해외 진출 – DISRUPT 100

“DISRUPT 100” 선정

DISRUPT 100 은 전세계 5백만개의 스타트업을 대상으로 그들이 보유한 잠재력과 시장 성장성을 고려하여 구글, 우버, 오라클, MS 등의 심사위원단이 선정



4. 양자산업을 위한 스타트업 육성

● 양자난수생성기 칩화 현황

- ✓ 양자산업은 세계 수준 5년 이상의 격차 있지만 양자난수생성기 칩화는 한국 기업 주도
- ✓ SK텔레콤, 이와이엘 칩화 성공 – 상용화 진행
- ✓ 스페인, 캐나다 연구기관 및 기업 칩화 연구 진행

● 문제점

- ✓ 한국은 대기업과 연구기관 주도로 진행되며 중소기업과 스타트업 기반이 매우 약함
- ✓ 국내 투자 환경 – 원천기술 보유 스타트업 투자 유치 어려움(단기성과 위주의 투자환경, 원천기술 투자 경험 부족)
- ✓ 타 국가 표준 선정 시 시장 진입 기회 상실 우려 → 이와이엘, 자체적으로 미국 NIST 등재 진행
- ✓ 기술을 가진 스타트업 위험 노출
 - 한국 기업들 보다 해외 정부기관과 기업에서 먼저 접촉, 기술협력 요청, 수출 및 기술이전 진행

● 정부 차원의 강력한 생태계 구축 지원 필요

- ✓ 양자기술 스타트업 선발, 집중적 관심과 자금 지원, 특별 규제 완화, 정부 주도의 기술 도입 필요
- ✓ 일반적 스타트업 지원 프로그램의 기준으로는 곤란
- ✓ 장기적 관점에서의 지원 절실, 원천 기술형 스타트업의 철저한 보호와 육성 필요 (先 육성, 後 평가)
- ✓ 향후 1~2년이 골든 타임, 국가 차원의 기회

Q & A



The First Quantum Security at Your Fingertips



토론자 약력

성 명	안 도 열	
소 속	서울시립대학교 전자전기컴퓨터공학부	
1. 학 력		
기 간	학 교 명	전 공 및 학 위
1979. 3~1983. 2	서울대학교	전자공학 (학사)
1983. 3~1985. 2	서울대학교	전자공학 (석사)
1985. 8~1988. 5	일리노이대학교 (UIUC)	전기공학 (박사)
2. 주 요 경 력		
기 간	기 관 명	직위, 직책
1988.8~1989.8	IBM T J Watson 연구소	연구원
1989.8~1992.4	포항공과대학	조교수
1992.1~1996.4	LG전자기술원	수석연구원
1996.3~현재	서울시립대학교	교수, 석좌교수
1998.10~2010.7	과기부 양자정보처리연구단	연구단장
2005.1~현재	미국 전기전자학회(IEEE)	펠로우
2009.1~현재	미국 물리학회(APS)	펠로우
2016.9~현재	일리노이대학 (UIUC)	Distinguished Alumni
2015.6~현재	(주)페타룩스	수상자 CEO

토론요약문

안 도 열

서울시립대 석좌교수, (주)페타룩스 대표

1. 주변강대국의 양자정보통신 투자현황
2. 양자암호: 광케이블 기반의 유선양자암호 및 위성기반의 자유공간 양자암호
Post Quantum Cryptography
3. 양자컴퓨팅: 어디까지? 현재 계획은 feasibility를 확인하는 수준
Logical Qubit vs Adiabatic Quantum Computation (AQC). Image
search, Vision, AI 등 최적화 문제 기반은 AQC도 좋은 대안임
4. 북한의 위협: 국가 프로젝트로 추진 중 (네이처 자매지 논문발표)

Plasmonics
DOI 10.1007/s11468-016-0481-1



Plasmonic Effect on the Optical Properties in a Hybrid V-Type Three-Level Quantum Dot-Metallic Nanoparticle Nanosystem

Myong-Chol Kim¹ · Nam-Chol Kim¹ · Song-Il Choe¹ · Gwang-Hyuk So¹ ·
Pong-Ryul Jang² · Yong-Jin Kim³ · Il-Gwang Kim⁴ · Jian-Bo Li⁴

✉ Nam-Chol Kim
ryongnam10@yahoo.com

¹ Faculty of Physics, Kim Il Sung University, Pyongyang, Democratic
People's Republic of Korea

² Scientific Experimental Apparatus Institute, Kim Il Sung
University, Pyongyang, Democratic People's Republic of Korea

³ Graduate School of Natural Science, Kim Il Sung University,
Pyongyang, Democratic People's Republic of Korea

⁴ Institute of Mathematics and Physics, Central South University of
Forestry and Technology, Changsha 410004, China

assisted Förster energy transfer [14], generation of a single
plasmon, induced exciton-plasmon-photon conversion, mod-
ifying the spontaneous emission in SQDs [10], the third-order
optical non-linearity [11, 12], etc. Recently, the research on
the optical non-linearity in a hybrid nanosystem has become
central topics, because of reporting the dark plasmon-exciton
hybridization which results in the enhancement of the light-
matter interaction and realization of the coherent optical con-
trol at the nanoscale [13–15]. More motivations have been
focused on the quantum plasmonics with the key technology
of manufacturing devices for quantum information processing
[16, 17] as single-photon transistors [18] or quantum switch
[19]. In particular, previous studies have shown the bistability

Acknowledgments This work was supported by the National Program
of DPR of Korea (Grant No. 131-00). This work was also supported by
the Human provincial National Science Foundation (Grant No. 14JJ3116)
and the National Natural Science Foundation of China (NSFC) (Grant
No. 11404410).

SCIENTIFIC REPORTS

SCIENTIFIC REPORTS

OPEN Plasmonic phase modulator based
on novel loss-overcompensated
coupling between nanoresonator
and waveguide

Received: 22 September 2015
Accepted: 20 November 2015
Published: 06 January 2016

Song-Seon Kim^{1,2}, Gyeom-Sang No¹, Da-Jin Yang^{1,2}, Zhong-Hua Han³, Li Zhou⁴, Nam-Chol Kim^{1,2},
Il-Gwang Kim³ & Guo-Qian Wang^{1,4}

한림원탁토론회는...

한림원탁토론회는 국가 과학기술의 장기적인 비전과 발전전략을 세우고, 동시에 과학기술 현안문제에 대한 해결방안을 모색하기 위한 목적으로 개최되고 있는 한림원의 대표적인 정책토론 행사입니다.

지난 1996년 처음 개최된 이래 지금까지 100여회에 걸쳐 초중등 과학교육, 문·이과 통합문제, 국가발전에 미치는 기초과학 등 과학기술분야의 기본문제는 물론 정부출연연구소의 발전방안, 광우병의 진실, 방사능, 안전 방제 등 국민생활에 직접 영향을 미치는 문제에 이르기까지 광범위한 주제를 다루고 있습니다.

한림원은 과학기술 선진화에 걸림돌이 되는 각종 현안문제 중 중요도와 시급성에 따라 주제를 선정하고, 과학기술 유관기관의 최고책임자들을 발제자로 초빙하여, 한림원 석학들을 비롯해 산·학·연·정의 전문가들이 심도 깊게 토론을 진행하고 있습니다.

토론결과는 책자로 발간, 정부, 국회와 관련기관에 배포함으로써 정책 개선방안을 제시하고 정책 입안자료를 제공하여 여론 형성에 기여하도록 힘쓰고 있습니다.

■ 한림원탁토론회 개최실적 (1996년 ~ 2017년) ■

회수	일 자	주 제	발제자
1	1996. 2. 22.	초중등 과학교육의 문제점	박승재
2	1996. 3. 20.	과학기술분야 고급인력의 수급문제	서정현
3	1996. 4. 30.	산업계의 연구개발 걸림돌은 무엇인가?	임효빈
4	1996. 5. 28.	과학기술 행정과 제도, 무엇이 문제인가?	박우희
5	1996. 7. 9.	연구개발 평가제도, 무엇이 문제인가?	강계원

회수	일 자	주 제	발제자
6	1996. 10. 1.	정부출연연구소의 역할과 기능에 대하여	김훈철
7	1996. 11. 4.	21세기 과학기술비전의 실현과 정치권의 역할	김인수
8	1997. 2. 25.	Made in Korea, 무엇이 문제인가?	채영복
9	1997. 4. 2.	산업기술정책, 무엇이 문제인가?	이진주
10	1997. 6. 13.	대학교육, 무엇이 문제인가?	장수영
11	1997. 7. 22.	대학원 과학기술교육, 무엇이 문제인가?	김정옥
12	1997. 10. 7.	과학기술 행정체제, 무엇이 문제인가?	김광웅
13	1998. 1. 22.	IMF, 경제위기 과학기술로 극복한다.	채영복
14	1998. 3. 13.	벤처기업의 활성화 방안	김호기, 김영대, 이인규, 박금일
15	1998. 5. 29.	국민의 정부의 과학기술정책	강창희
16	1998. 6. 26.	정보화시대의 미래와 전망	배순훈
17	1998. 9. 25.	과학기술정책과 평가제도의 문제	박익수
18	1998. 10. 28.	경제발전 원동력으로서의 과학기술의 역할	김상하
19	1999. 2. 12.	21세기 농정개혁의 방향과 정책과제	김성훈
20	1999. 3. 26.	지식기반 경제로의 이행을 위한 경제정책 방향	이규성
21	1999. 5. 28.	과학기술의 새천년	서정옥
22	1999. 9. 10.	신 해양시대의 해양수산정책 발전방향	정상천
23	2000. 2. 10.	21세기 환경기술발전 정책방향	김명자
24	2000. 4. 14.	경제발전을 위한 대기업과 벤처기업의 역할	김각중

회수	일 자	주 제	발제자
25	2000. 6. 16.	과학·기술발전 장기 비전	임 관
26	2000. 9. 15.	국가 표준제도의 확립	김재관
27	2000. 12. 1.	국가 정보경쟁력의 잣대: 전자정부	이상희
28	2001. 5. 4	환경위기 극복과 지속가능 경제발전을 위한 과학 기술개발전략	박원훈, 류순호, 문길주, 오종기, 한무영, 한정상
29	2001. 7. 18	국가 과학기술발전에 미치는 기초과학의 영향	임관, 명효철, 장수영
30	2001. 9. 21	산업계에서 원하는 인재상과 공학교육의 방향	임관, 한송엽
31	2001. 10. 31	적조의 현황과 앞으로의 대책	홍승룡, 김학균
32	2001. 12. 5	광우병과 대책	김용선, 한홍율
33	2002. 7. 19	첨단기술 (BT,ET,IT,NT)의 실현을 위한 산업화 대책	한문희, 이석한, 한송엽
34	2002. 9. 13	우리나라 쌀 산업의 위기와 대응	이정환, 김동철
35	2002. 11. 1	생명윤리 - 과학 그리고 법: 발전이나 규제냐?	문신용, 이신영
36	2003. 3. 14	과학기술분야 졸업생의 전공과 직업의 연관성	조황희, 이만기
37	2003. 6. 18	국내 농축산물 검역현황과 발전방안	배상호
38	2003. 6. 27	대학과 출연연구소간 연구협력 및 분담	정명세
39	2003. 9. 26	그린에너지 기술과 발전 방향	손재익, 이재영, 홍성안
40	2004. 2. 20	미래 고령사회 대비 국가 과학기술 전략	오종남
41	2004. 10. 27	고유가시대의 원자력 이용	정근모
42	2004. 12. 7	농산물 개방화에 따른 국내 고추산업의 현황과 발전전략	박재복
43	2005. 9. 30	과학기술윤리	송상용, 황경식, 김환석

회수	일 자	주 제	발제자
44	2005. 11. 25	과학기술용어의 표준화 방안	지제근
45	2005. 12. 1	융합과학시대의 수학의 역할 및 수학교육의 방향	정근모, 최형인, 장준근
46	2005. 12. 15	해양바이오산업, 왜 중요한가?	김세권, 김동수
47	2006. 11. 7	첨단과학시대의 교과과정 개편방안	박승재
48	2006. 12. 22	과학기술인 복지 증진을 위한 종합 대책	설성수
49	2007. 6. 29	선진과학기술국가 가능한가? - Blue Ocean을 중심으로	김호기
50	2007. 11. 9	우리나라 수학 및 과학교육의 문제점과 개선방향	김도한, 이덕환
51	2008. 5. 9	태안반도 유류사고의 원인과 교훈	하재주
52	2008. 5. 8	광우병과 쇠고기의 안전성	이영순
53	2008. 6. 4	고병원성조류인플루엔자(AI)의 국내외 발생양상과 우리의 대응방안	김재홍
54	2008. 10. 8	High Risk, High Return R&D, 어떻게 해야 하는가?	김호기
55	2008. 11. 11	식량위기 무엇이 문제인가?	이정환
56	2008. 12. 11	초중고 수학 과학교육 개선방안	홍국선
57	2008. 12. 17	우리나라 지진재해 저감 및 관리대책의 현황과 개선방안	윤정방
58	2009. 2. 19	21세기 지식재산 비전과 실행 전략	김영민
59	2009. 3. 31	세계주요국의 나노관련 R&D 정책 및 전략분석과 우리의 대응전략	김대만
60	2009. 7. 20	국가 수자원 관리와 4대강	심명필
61	2009. 8. 28	사용후핵연료 처리 기술 및 정책 방향	송기찬, 전봉근
62	2009. 12. 16	세종시와 국제과학비즈니스벨트	이현구

회수	일 자	주 제	발제자
63	2010. 3. 18	과학도시와 기초과학 진흥	김중현
64	2010. 6. 11	지방과학기술진흥의 현황과 과제	정선양
65	2011. 2. 28	국제과학비즈니스벨트와 기초과학진흥	민동필, 이충희
66	2011. 4. 1	방사능 공포, 오해와 진실	기자회견
67	2012. 11. 30	융합과학/융합기술의 본질 및 연구방향과 국가의 지원시스템	이은규, 여인국
68	2013. 4. 17	한미원자력협정 개정협상에 거는 기대와 희망	문정인
69	2013. 6. 11	통일을 대비한 우리의 식량정책 이대로 좋은가?	이철호
70	2013. 7. 9	과학기술중심사회를 위한 과학기술원로의 역할과 의무	이원근
71	2013. 7. 22	대학입시 문·이과 통합, 핵심쟁점과 향후 과제는?	박재현
72	2014. 1. 17	국가안보 현안과제와 첨단과학기술	송대성
73	2014. 3. 4	융합과학기술의 미래 - 인재교육이 시작이다	강남준, 이진수
74	2014. 5. 9	과학기술연구의 새 지평 젠더혁신	이혜숙, 조경숙, 이숙경
75	2014. 5. 14	남북한 산림협력을 통한 한반도 생태통일 방안은?	김호진, 이돈구
76	2014. 5. 22	창조경제와 과학기술	이공래, 정선양
77	2014. 5. 29	재해·재난의 예방과 극복을 위한 과학기술의 역할은?	이원호, 윤정방
78	2014. 6. 10	벼랑 끝에 선 과학·수학 교육	정진수, 배영찬
79	2014. 6. 14	문학과 과학, 그리고 창조경제	정종명, 최진호
80	2014. 6. 25	‘DMZ세계평화공원’과 남북과학기술협력	정선양, 이영순, 강동완
81	2014. 7. 24	국내 전통 발효식품산업 육성을 위한 정책 대안은?	신동화

회수	일 자	주 제	발제자
82	2014. 9. 17	'과학기술입국의 꿈'을 살리는 길은?	손경한, 안화용
83	2014. 9. 30	한국 산업의 위기와 혁신체제의 전환	이 근
84	2014. 11. 14	경제, 사회, 문화, 산업 인프라로서의 사물인터넷(IoT): 그 생태계의 실현 및 보안방안은?	김대영, 김용대
85	2014. 11. 28	공유가치창출을 위한 과학기술의 나아갈 길은? 미래식품과 건강	권대영
86	2014. 12. 5	창발적 사고와 융합과학기술을 통한 글로벌 벤처 생태계 조성 방안	허석준, 이기원
87	2015. 2. 24	구제역·AI의 상재화: 정부는 이대로 방치할 것인가?	김재홍
88	2015. 4. 7	문·이과 통합 교육과정에 따른 과학·수학 수능개혁	이덕환, 권오현
89	2015. 6. 10	이공계 전문가 활용 및 제도의 현황과 문제점	이건우, 정영화
90	2015. 6. 25	남북 보건의료 협정과 통일 준비	신희영, 윤석준
91	2015. 7. 1	메르스 현황 및 종합대책	이종구
92	2015. 7. 3	'정부 R&D 혁신방안'의 현황과 과제	윤현주
93	2015. 9. 14	정부 R&D예산 감축과 과학기술계의 과제	문길주
94	2015. 10. 23	사회통합을 위한 과학기술 혁신	정선양, 송위진
95	2015. 11. 4	생명공학기술을 활용한 우리나라 농업 발전방안	이향기, 박수철, 곽상수
96	2015. 11. 9	유전자가위 기술의 명과 암	김진수
97	2015. 11. 27	고령화사회와 건강한 삶	박상철
98	2015. 12. 23	따뜻한 사회건설을 위한 과학기술의 역할: 국내외 적정기술을 중심으로	박원훈, 윤제용
99	2016. 2. 29	빅데이터를 활용한 의료산업 혁신방안은?	이동수, 송일열, 유회준
100	2016. 4. 18	대한민국 과학기술: 미래 50년의 도전과 대응	김도연

회수	일 자	주 제	발제자
101	2016. 5. 19	미세먼지 저감 및 피해방지를 위한 과학기술의 역할	김동술, 박기홍
102	2016. 6. 22	과학기술강국, 지역 혁신에서 답을 찾다	남경필, 송종국
103	2016. 7. 6	100세 건강과 장내 미생물 과학! 어디까지 왔나?	김건수, 배진우, 성문희
104	2016. 7. 22	로봇 기술과 미래	오준호
105	2016. 8. 29	융합, 융합교육 그리고 창의적 사고	김유신
106	2016. 9. 6	분노조절장애, 우리는 얼마나 제대로 알고 있나?	김재원, 허태균
107	2016. 10. 13	과학기술과 미래인류	이광형, 백종현, 전경수
108	2016. 10. 25	4차 산업혁명시대에서 젠더혁신의 역할	이우일, 이혜숙
109	2016. 11. 9	과학기술과 청년(부제: 청년 일자리의 현재와 미래)	이영무, 오세정
110	2017. 3. 8	반복되는 구제역과 고병원성 조류인플루엔자, 정부는 이대로 방치할 것인가?	류영수, 박최규
111	2017. 4. 26	지속가능한 과학기술 혁신체계	김승조, 민경찬
112	2017. 8. 3	유전자교정 기술도입 및 활용을 위한 법·제도 개선방향	김정훈
113	2017. 8. 8	탈원전 논란에 대한 과학자들의 토론	김경만, 이은철, 박홍준
114	2017. 8. 11	새롭게 도입되는 과학기술혁신본부에 바란다	정선양, 안준모

[illegible]

[illegible]

www.kast.or.kr

본 사업은 과학기술진흥기금 및 복권기금의 지원으로 시행되고 있습니다.