글로벌 ICT 표준 컨퍼런스 2023

Global ICT Standards Conference 2023

(세션1) 양자기술: 디지털 세상의 새로운 패러다임

新산업 창출 및 국민안심 서비스 제공을 위한 양자정보통신 표준화 로드맵

권대성 연구위원, ETRI 부설 연구소

주최 과학기술정보통신부 Ministry of Science and ICT, 특허청 Korean Intellectual Property Office
주관 국립전파연구원 National Radio Research Agency, TTA, IITP, KEA, kista, ETRI

Index

00. 발표 요약

본 발표에서는 양자정보통신 분야에서 국제표준 선점을 위한 중장기 전략을 제시

이를 위하여, 양자정보통신 기술/표준화 현황,

표준화 필요 기술을 찾기 위한 표준 구조 모델 적용과정,

구조 모델 적용을 통한 표준 R&D 대상 기술 선정과

표준 R&D 대상 선정 기술의 중장기 로드맵을 소개

중장기 로드맵은

- 양자암호통신 확대를 위한 요소기술 표준화,
- 양자컴퓨팅 활용의 기반이 되는 성능 및 검증기술 표준화,
- 양자 센서 성능 검증에 필수적인 측정 기술 표준화,
- 양자 네트워크 표준 선점을 위한 전략적 표준 확보

등으로 구성

01. 개요 및 현황

양자정보통신

양자정보통신은 양자역학적 특성(중첩, 얽힘, 비가역성, 불확정성)을 가진 양자를 정보통신에 적용하기 위한 기술로,

- 양자의 도청 불가능성을 이용한 양자암호통신,
- 양자의 중첩된 데이터의 병렬적 처리가 가능한 양자 컴퓨팅,
- 센싱·계측 기술의 분해능, 민감도 및 측정을 대폭 향상시킬 수 있는 양자 센싱,
- 양자 디바이스 간의 양자 정보 전송을 위한 양자 네트워크 기술로 구성

* 중첩(superposition): 0과 1이 공존
* 얽힘(entanglement): (거리 무관) 양자쌍에 대한 특수 상관관계
* 비가역성(irreversibility): 확정된 값은 다시 되돌릴 수 없음, 복제 불가
* 불확정성(uncertainty): 교환 가능하지 않은 두 물리량(예: 위치와 운동량)을 동시에 측정할 수 없음

01. 개요 및 현황

국내 기술 현황

- 양자통신, 양자컴퓨터, 양자 센서에 대한 정부 차원의 전략적 투자 확대 및
  국외 참조 기술의 비약적 진화, 産·學·硏의 적극적 참여로 양자 기술 부흥기 도래
  - 양자컴퓨터는 혁신적인 초고속 컴퓨팅 환경을 제공하고,
    양자센서는 비약적 초정밀 센싱을 가능하게 하며,
    양자통신은 양자기기 간 연결을 제공하여 과학기술 및 ICT의 혁신을 초래 가능

- 양자암호통신은 통신의 도청 위험성을 원천적으로 제거하여 보안기술의 안전성을
  획기적으로 개선하는 이점으로, 기술 실용화 및 시장 확보에 주력
  - 양자암호통신 중 QKD는 '20년 상용화에 성공한 첫 사례로, SKT와 KT를 중심으로 국내 시장을 선도 중
  - QKD의 적용 확대를 위한 무선 QKD, 소형화를 위한 QKD 양자광학계 칩 기술,
    암호키 대신 메시지 전송을 위한 직접통신 기술 확보 중

- 양자정보통신 전반적으로 글로벌 기술 선도를 위하여 출연연 및 주요 대학을 중심으로
  핵심 원천기술 확보를 위하여 노력 중
  - 양자 컴퓨팅 HW, 양자 알고리즘 및 양자정보이론, 양자센싱, 양자 네트워크 대규모 연구 진행 중

01. 개요 및 현황

국외 기술 현황(1/2)

- 양자 기술을 과학기술과 ICT의 혁신 기술로 인식하여 미·중 기술 패권 경쟁이 심화되고 있으며, 유럽, 일본 등 국가 차원의 투자 및 기술 개발 활발히 진행 중
  - 미국은 관련 법제정, 전담기구 설치, 국가전략 수립 등으로 리더십을 유지하기 위한 노력 중이며, 중국은 국가 차원의 연구조직 결집 및 집중 투자로 미국을 앞서기 위한 기술 확보에 주력

- 양자암호통신 기술은 상용화를 위한 기술 성숙도 제고 및 시험평가 준비가 글로벌 기업 중심으로 진행되고 있으며, 글로벌 네트워크 구축을 위한 인공위성 양자암호통신, 상호연동 기술 개발이 활발히 진행 중
  - 해외 글로벌 기업들이 적극적으로 QKD 기술 연구 프로그램을 진행해오고 있으며, 중국을 시작('16)으로 양자 위성통신 기술 연구도 활발히 진행 중
  - 유럽은 EuroQCI(European Quantum Communication Infrastructure) 계획 아래 산·학·연(총 38개)이 참여하여 QKD 장비를 연결하는 OPENQKD PROJECT 시작('19)

- 양자 네트워크 기술은 차세대 국가 사회경제 플랫폼으로 예상되어 세계적으로 국가 정책 및 기술개발 방향성을 양자 인터넷 구현에 맞추고 기술력 확보 노력

01. 개요 및 현황

국외 기술 현황(2/2)

- 가장 파급력이 크고 기술 경쟁이 심한 분야는 컴퓨팅의 혁신을 가져올 수 있는 양자컴퓨팅 기술 분야로, 거대 IT 기업과 양자컴퓨팅 전문 스타트업을 중심으로 치열한 범용 양자컴퓨터 연구개발 경쟁 중
  - 거대 IT 기업(IBM, Google, Intel, 알리바바 등)과 양자컴퓨팅 전문 스타트업(Rigetti, IonQ, Xanadu, PsiQuantum, ORCA, D-Wave 등)을 중심으로 양자컴퓨터 구현 연구 진행 중
  - 슈퍼컴퓨터 대비 양자컴퓨터의 효용성 입증이 가능한 '양자 우위(Quantum Supremacy)'는 구글, 중국과학기술 대학 등 시연 성공('19년)
  - 미국, 유럽 중심으로 시뮬레이터 컴퓨터 관련 문제기술 확보 및 문제 해결 연구도 활발히 진행 중

- 양자센서는 미국 및 유럽을 중심으로 기존 센서의 한계를 양자를 적용하여 극복하는 연구가 활발히 진행 중으로 다수의 상용화 솔루션 개발 중
  - 미국, 프랑스에서는 소형화와 집적화를 통해 실용성을 높이는 원자 기반 중력·가속도 센서 (ex. MuQuans, 2018~) 및 칩스케일 원자시계 개발 (NIST, 2001~ & Microsemi, 2018~)
  - 미국, EU, 영국, 스위스에서는 다이아몬드 색중심 양자센서의 소재, 광·마이크로웨이브 제어, 응용 기술을 개발하여 다수의 상용화 솔루션 발표 (ex. Lockheed Martin, 2019~)
  - 미국 등에서는 원자 증기셀을 이용하는 자기장 및 고주파 전기장 센서 응용기술 개발과 사업화 추진 (NIST & Rydberg Technologies, 2018~)

01. 개요 및 현황

국내단체표준(TTA)

- 양자통신 프로젝트 그룹(PG225)
  - (역할) 양자키 분배망 및 연동 요구사항 및 아키텍쳐 기술, 서비스품질 보장 기술 관련 표준화 담당
  - (주요내용) 양자키 분배망 기관 도입 시 필요한 운영 지침 및 사례에 대한 표준 진행
- 정보보호 기반 프로젝트 그룹(PG501)
  - (역할) 암호 알고리즘/프로토콜, 양자정보통신의 암호키 관리, 암호응용기술 관련 표준화 담당
  - (주요내용) 2018년 양자 키 분배 기술에 대해 일반적인 모델과 절차 및 양자키분배 프로토콜인 BB84 프로토콜에 대한 절차 관련 표준 제정 완료
- 응용보안/평가인증 프로젝트 그룹(PG504)
  - (역할) 공통평가기준(CC), 암호모듈 검증(KCMVP) 등 보안성 인증 및 평가 기술 관련 표준화 담당
  - (주요내용) 양자 키분배 시스템의 안전성을 보장하기 위한 요구사항 표준이 제정('19년)되었고, 현재 양자 키 분배 장비 보안 요구사항 확인을 위한 시험 방법 표준이 과제 채택되어 진행 중('23년)
- 미래양자융합포럼
  - (역할) 양자 분야의 산·학·연 교류를 통해 양자 분야 생태계 활성화를 촉진하기 위한 포럼
  - (주요내용) TTA PG225와의 협업(간사)을 통해 양자키 분배망 관련 표준 공동 개발 중, 양자암호통신 표준 거버넌스를 위한 특별위원회 설치

01. 개요 및 현황

미래양자융합포럼 – 양자암호통신 표준화 특별 위원회

- 양자암호통신 분야에서, 실용화의 기준이 표준을 중심으로 글로벌 리더쉽 확보를 위한 産·學·硏·官 협력 체계

01. 개요 및 현황

국제공식표준

- ITU-T
  - SG11(Protocols, testing & combating counterfeiting): 양자키분배망의 신호 방식을 위한 프로토콜 구조 및 응용제어, 세션 및 접속제어 등 의 표준 개발 중
  - SG13(Future networks): 34건의 양자암호 네트워크 표준 개발 중이며, 양자 네트워크 분야로 확장 예정
  - SG17(Security): QKD 네트워크 보안 요구사항, 키 관리 보안 요구사항, 신뢰노드에 대한 보안 요구사항 표준 진행 중
- ISO/IEC JCT 1(Joint Technical Committee)
  - SC27(Information security, cybersecurity and privacy protection): IT 보안제품 공통평가기준(CC)를 기반으로 양자키분배 장치의 보안 요구사항과 시험 방법 표준 개발 중
  - WG14(Quantum Information Technology): 양자 컴퓨팅 용어 및 개념, 양자 머신 데이터셋, 양자자원 분석 플랫폼 관련 표준 개발 중
- IEC
  - TC90(Superconductivity): 초전도 나노선 단광자검출기(SNSPD) 암전류 및 조셉슨 접합 시험 평가 표준 제정
  - SEG 14(Quantum technologies): JTC-QT 설립 추진 중, JTC 1과의 관계 정립 및 QIT분야와의 역할 구분 필요

01. 개요 및 현황

국제사실표준

- ETSI
  - ISG QKD(Quantum Key Distribution)
    - QKD 보안 요구사항과 관련하여 광학계, Security Proof, QKD 공통평가기준 (Common Criteria) 및 QKD 네트워크 관리를 위한 SDN (Software Defined Network) 등 에 대한 표준 개발 중
- IEEE
  - 양자컴퓨팅 용어(P7130), 성능 지표 및 벤치마크(P7131), 아키텍쳐(P3120), 알고리즘 개발 (P2995), 시뮬레이터 (P3120.1) 등에 관한 표준 개발 중
- IRTF
  - QIRG(Quantum Internet)
    - 양자 인터넷 구조원리(Architecture Principle for a Quantum Internet)에 대한 표준 제정('23.3) 및 응용시나리오(Application Scenarios for the Quantum Internet) 표준 개발 중

02. 표준 구조 모델

표준 구조 모델 개발 방법론

- (분류체계 후보군 조사) 타기관 로드맵, 백서 및 해외(유럽) 기술 로드맵 등에서 정의한 양자정보통신 분류체계 참조

  * IITP 기술로드맵 및 R&D 기술 분류체계, NIA 양자정보기술백서, 유럽 양자선언문(로드맵), ETRI, KISTEP 양자통신 관련 자료 등
  * '양자정보통신'은 Ver.2023 전략맵 신규 분과로, 분과 신설시 논의한 중분류 참조

- (기술 현황 분석) 양자정보통신 기술 특성상 각 영역별 특성(양자컴퓨팅, 센싱 등)이 상이한 점을 고려하여 Top-down 방식으로 기술 세부 분류 개발

영역	특성
양자암호통신	양자역학적 특성(얽힘, 비가역성, 불확정성), 네트워크과 보안기술 특성 결합
양자컴퓨팅	양자역학적 특성을 지닌 HW 구성, 컴퓨팅 활용을 위한 SW, 알고리즘 필요
양자센싱	활용 분야에 따른 양자 소자 및 측정 기술의 다양성
양자네트워크	양자기기(양자컴퓨터, 양자센서 등) 간 양자 정보를 전달하는 기술

- (표준-기술 간 체계 조정) 국내·외 표준화 현황 분석을 통한 기술 간 분류체계 갭 차이를 조정하여 Bottom-up 방식으로 분류체계 확정

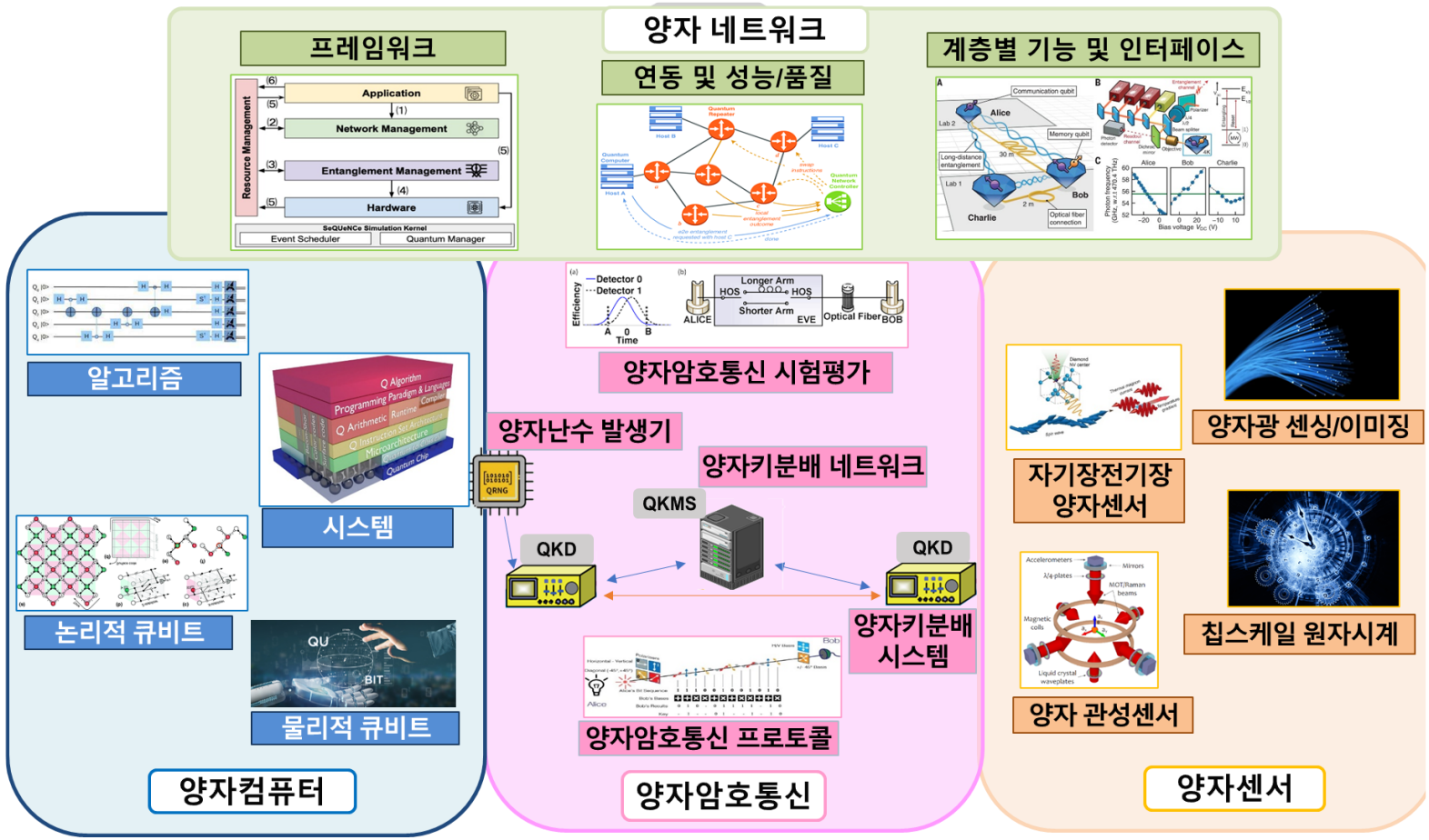
02. 표준 구조 모델

표준 구조 모델 구성

- 레벨1: 양자암호통신, 양자 컴퓨팅, 양자센싱, 양자네트워크
- '양자암호통신'은 기술적, 표준 부분에서 가장 활발히 개발된 영역으로, 기술적 그룹화를 통해 분류함
  - 양자암호통신 프로토콜/양자키분배 시스템/양자키분배 네트워크/양자난수발생기/양자암호통신 장비·서비스 시험 평가
- '양자컴퓨팅'은 컴퓨팅 구성 기술에 따라 분류하고, 컴퓨팅 기술을 포괄하고 정의하는 부분(개념 및 정의)을 추가
  - 개념 및 정의/물리 큐비트/논리 큐비트/시스템/알고리즘
- '양자 센싱'은 센서의 종류에 따라 분류함
  - 양자 관성센서/침스케일 원자시계/자기장·전기장 양자센서/양자광 센싱·이미징
- '양자네트워크'는 네트워크 구성 요소 기술에 따라 분류함
  - 프레임워크/계층별 기능 및 인터페이스/연동 및 성능·품질

02. 표준 구조 모델

표준 구조 모델 구성



02. 표준 구조 모델

양자암호통신 요소 기술 및 표준화 현황

구분				"표준화 특성"					
분류1	분류2	분류3	분류4	개념/정의	요구사항/유즈케이스	참조구조/기능도출	데이터포맷/스키마	프로토콜/인터페이스	시험/가이드라인
양자암호통신	양자암호통신 프로토콜	QKD 프로토콜		(TTA)	(ISG QKD)			(TTA)	
		QKD 프로토콜 이론적 안전				(ISG QKD)			
		양자 보안 프로토콜	양자인증						
			양자서명						
			양자 비밀공유		(ITU-T)				
			양자 직접통신						
	양자키분배 시스템	QKD 광학계				(TTA)			
		QKD 후처리 기술							
		QKD 인터페이스		(ISG QKD)				(TTA)	
		QKD 시스템 제어							
	양자키분배 네트워크	양자키 관리			(ITU-T)	(ITU-T)		(TTA) 2019-	
		QKD 네트워크 프로토콜		(TTA)	(TTA)	(TTA)		(TTA)	
		QKD 신뢰노드			(ITU-T)				
		QKD 이기종 간 연동 기술		(ITU-T)	(ITU-T)	(ITU-T)		(TTA) 2022-	
		QKD 네트워크 관리 및 양자		(ITU-T)	(TTA)	(ITU-T),		(ISG QKD)	(ITU-T)
	양자난수발생기	양자 난수 발생 기술				(ITU-T)			
		양자 난수 검증							
	양자암호통신 장비/서비스 시험평가	양자암호 품질평가		(ISG QKD)				(ISG QKD)	(ITU-T)
		QKD 광학계 양자성 시험						(ISG QKD)	
		QKD 장비 안전성 검증			(TTA)				(TTA)
		QKD 부채널 위협 대응 기술							

02. 표준 구조 모델

양자컴퓨팅 요소 기술 및 표준화 현황

구분				"표준화 특성"					
분류1	분류2	분류3	분류4	개념/정의	요구사항/유즈케이스	참조구조/기능도출	데이터포맷/스키마	프로토콜/인터페이스	시험/가이드라인
양자컴퓨팅	개념 및 용어			(JTC1)					
	물리 큐비트	물리 큐비트 및 양자 게이트							
		다중 양자 프로세서 모듈 간							
		양자 프로세서 제어							
		물리 양자 게이트 컴파일							
		물리 큐비트 오류 완화							
		물리 큐비트 및 게이트 성능							
	논리 큐비트	양자오류 정정							
		논리 큐비트 블럭 및 게이트							
		논리 양자 게이트 컴파일							
		특수목적 논리 큐비트 생성							
		논리 큐비트 및 게이트 성능							
	시스템	양자컴퓨팅 시스템 구조				(IEEE) IEEE			
		양자 데이터 이동							
		양자 데이터 인코딩							
		양자컴퓨팅 언어	프로그래밍 언어						
			시스템 내부 언어						
		시스템 수준에서의 양자컴							(IEEE) IEEE
	알고리즘	기본연산 라이브러리				(IEEE) IEEE			
		잡음 감수 알고리즘(NISQ)							
		오류 내성 알고리즘(FTQC)							
		알고리즘 성능 정의 및 검증							

02. 표준 구조 모델

양자센싱 요소 기술 및 표준화 현황

구분				"표준화 특성"					
분류1	분류2	분류3	분류4	개념/정의	요구사항/유즈케이스	참조구조/기능도출	데이터포맷/스키마	프로토콜/인터페이스	시험/가이드라인
양자센싱	양자 관성 센서	원자 간섭신호 생성 기술							
		레이저 냉각/포획 기술							
		라만 레이저 광회로 집적 기							
		나노역학계 냉각 기술							
		광역학계 잡음 측정 기술							
	칩스케일 원자시계	원자 증기셀 소형화 기술							
		광주파수 합성 기술							
		광회로 집적화 기술							
		양자 기반 시간 동기화 기술							
	자기장·전기장 양자센서	원자 전기장 측정 기술	원자 저주파 전기장 측정 기						
			원자 고주파 전기장 측정 기						
		양자 단일/복합 점결함 생성							
		고체 점결함 자기장 측정 기술	고체 점결함 스핀 DC 자기						
			고체 점결함 AC 자기장 측						
		나노 SQUID 기반 자속 측정							
		원자자력계	SERF 기반 원자자력계						
			Total field 원자자력계						
			RF 원자자력계						
		파라메트릭 증폭기 기술							(IEEE/IEC)
	양자광 센싱/이미징	양자분광센서 기술							
		고분해능 양자현미경 기술							
		압착광원 기반 저잡음 간섭							
		양자 조명 이미징 기술							
		초전도나노선 단광자측정기							(IEEE/IEC)

02. 표준 구조 모델

양자네트워크 요소 기술 및 표준화 현황

구분				"표준화 특성"					
분류1	분류2	분류3	분류4	개념/정의	요구사항/유즈케이스	참조구조/기능도출	데이터포맷/스키마	프로토콜/인터페이스	시험/가이드라인
양자네트워크	프레임워크	양자 네트워크 프레임워크		(ITU-T)	(IRTF QIRG)				
		양자 네트워크 프레임워크							
		양자 네트워크 프레임워크							
	계층별 기능 및 인터페이스	전송 계층	양자 얽힘 생성·분배						
			양자 네트워크 전송 계층 오						
			양자 전송 프로토콜			(TTA)			
			중계기/메모리						
		네트워킹 계층	양자 전송 스위칭 프로토콜						
			라우팅 프로토콜						
			큐잉 및 버퍼링 알고리즘						
		제어/관리 계층	양자 네트워크 장애(fault)						
			성능 (Performance)						
			구성 (Configuration)						
		인터페이스	양자 네트워크 계층 내 기						
			계층간 인터페이스						
			연동 인터페이스						
	연동 및 성능/품질	연동	양자 네트워크 연동구조(이						
			연동 기능 요구사항						
		성능	양자 네트워크 망 성능 파라		(TTA)				
			네트워크 성능 파라미터별						
		품질	양자 네트워크 서비스 품질		(TTA)				
			서비스 품질 파라미터별 기						

02. 표준 구조 모델

표준 발전 전망(1/2)

- (국제 표준화 발전 전망) ISO/IEC JTC1/JTC-QT, ETSI ISG QKD, ITU-T 중심으로 양자암호통신을 비롯한 양자 네트워크 및 인터넷 관련 표준이 지속적으로 활발하게 진행될 전망
  - QKD 네트워크/양자키 관리 계층 등에 대한 표준이 활발히 진행 중이며, QKD 중 표준이 없는 기술인 QKD 후처리/광학계 등에 대한 표준, 양자 네트워크를 위한 양자 인증/서명에 대한 표준화도 활발히 진행될 전망
  - 양자컴퓨팅 기술 개발을 견인하고, 양자컴퓨팅의 우월성을 입증하기 위한 표준화 필요성 확대
  - 양자센싱 기술은 메트롤로지 연구개발 체계에 기반한 측정표준 논의를 중심으로, 기술 발전과 응용 확대에 따른 표준화 노력이 증가할 것으로 전망
    * 유럽메트롤로지 연구사업(EMPIR)과 같은 국제공동연구 프로그램을 통해 다양한 양자센싱 및 계측 기술들이 개발되고 있으며, 기존 도량형 측정표준 향상과 ETSI 등과의 협력 아래 양자정보통신 표준화를 위한 측정 모범사례 가이드(best practice guide) 제공을 목표로 진행 중
  - 양자 네트워크는 통신 인프라로서 IETF, IRTF, ITU-T 등에서 네트워킹용 표준과 미래 통신망 관련 표준이 더욱 확대 진행될 것으로 전망

02. 표준 구조 모델

표준 발전 전망(2/2)

- (국내 표준화 발전 전망) 양자암호통신 및 양자통신 관련 표준화가 정부의 정책적 지원으로 TTA를 중심으로 활발히 전개될 예정이며, 양자컴퓨팅 및 양자센서 기술 개발 활성화에 따른 국내 표준화 수요들이 증가 전망
  - 양자암호통신은 QKD 프로토콜 및 QKD 장비의 안전성 평가를 위한 요구사항 표준화가 TTA에서 진행되어 '23년 시행의 QKD 장비 국가 인증 정책에 반영되었고(1단계,2~3단계 기술/기준/표준 확보 필요), 향후 QKD 네트워크와 관련된 표준이 국제표준에 이어 국내에서도 활발히 진행될 것으로 전망
  - 양자컴퓨팅 및 양자 센싱 분야는 TTA 등을 중심으로 글로벌 경쟁을 위해서 국제표준을 적극 준용하는 한편, 국제 표준화 제정에 국내 연구 종사자들의 요구사항 반영 노력 필요

    * 양자 하드웨어/소프트웨어(양자컴퓨팅, 양자센싱) 등 전반적인 내용을 다루는 PG 신설 필요
  - 양자 네트워크는 양자암호통신 국내 표준화 경험을 바탕으로 착수되고 있으며, 우선은 IRTF나 ITU-T SG13의 국제표준을 국내표준으로 준용하는 방향으로 진행할 것으로 전망

02. 표준 구조 모델

시사점(1/2)

- QKD 기술이 개발되어 보급 활성화되고 있지만, 주로 네트워크 관점의 표준화가 주를 이루고 있어,
  안전성 확보/연동을 위한 표준화가 시급함
  - QKD 프로토콜은 표준 없이 사용되어 통용되어 온 영역으로 장비 인증 및 표준화된
    프로세스 정립에 어려움이 있어 표준화가 필요
  - QKD 기술은 현재 제조사나 통신사, 국가가 다를 경우 양자암호 통신망 연결이
    불가능하여 서로 다른 QKD 기술로 구현된 QKD 장비 간 연동 기술 개발이 필요
  - 양자 네트워크 및 양자 인터넷 환경에서 QKD가 제공하지 못하고,
    QKD를 비롯한 양자 네트워크 보안에 반드시 필요한 양자인증 표준 필요
  - 한국이 선도하고 있는 QKD 시험/검증 정책의 지속적인 리더쉽 확보를 위해서는
    현재 기본적인 양자성 평가에서/종합적인 양자 안전성을 시험/평가할 수 있는 기술 및 표준 확보 필요
- 양자컴퓨팅 SW/HW 기술에 대해서, 엄격한 성능 검증이 요구되나
  현재는 연구개발 초기 단계로 다양한 방식으로 성능이 평가되어 보고되고 있지만,
  향후 엄격하고 공정한 성능 분석 및 비교를 위해 표준화된 방법 필요

02. 표준 구조 모델

시사점(2/2)

- 양자센싱기술 중 상용화가 임박한 다이아몬드 등의 고체 점결함의 양자 상태를 이용한 광학적 자기장 측정 기술의 활용을 위한 센서의 성능에 관한 시험 평가 표준화 필요
  - 나노해상도 수준의 자기장, MRI 측정 이미징에 활용되는 단일 NV센터의 민감도와 분해능을 측정하는 시험평가 표준 필요
  - 범용 자기장 측정 센서 모듈로서 활용되는 앙상블 NV센터의 민감도와 유효 센서 크기를 규정하는 시험평가 표준 필요
- 양자 디바이스의 자원 간의 네트워킹을 제공하는 양자 네트워크 개발을 위해서는 이를 전반적으로 조망할 수 있는 참조 모델 및 네트워크에서 양자 전송에 필요한 양자 오류 정정기술에 대한 표준화 필요
  - 양자 디바이스 (양자 컴퓨터, 양자 센서, 양자키분배 장치 등)의 자원공유 및 가치제고를 위해 상호간 비용효율적 네트워킹을 제공하는 양자 네트워크 기술 개발 필요하며, 이를 전반적으로 조망할 수 있는 참조 모델 표준 필요
  - 양자네트워크 기반의 양자암호통신은 양방향 송수신 기술로서 수신자가 송신자의 통신방식 (특히 오류정정을 위한 사전 부호화 방식)을 사전에 공유하고 있어야 양자상태를 수신 후 오류 정정 할 수 있으며 이에 대한 표준 필요

02. 표준 구조 모델

비전, 목표, 추진 전략

비전	표준화 초기단계인 양자정보통신 분야에서 국제표준 선점을 통한 양자정보통신 분야 기술 선도

		~2024	~2026	~2028
목표		○ 양자암호통신 표준 선도 ○ 양자컴퓨팅, 센싱 표준 요소기술 확보 ○ 국내 전담표준기구 설립	○ 양자인터넷 표준선도 ○ 양자컴퓨팅, 센싱 종합적 표준확보전략 수립 ○ 국가 간 표준협력 전략	○ 양자정보통신 표준선도 ○ 양자정보통신 시장 선도 ○ 글로벌 표준협력 전략
추진전략	정책/제도	○ 양자 기술개발, 인재양성, 기반 인프라 투자 ○ 도입/확산정책 시행	○ 양자기술 활용을 위한 산업 생태계 조성 ○ 실용화를 위한 표준개발 활성화 정책 시행	○ 양자 인터넷 도입기반 마련 ○ 양자기술 전반에서 국제 표준 리더쉽 확보
	기술개발	○ 양자컴퓨팅, 센서, 인터넷 투자 확대 ○ 양자암호통신 실용기술 확보 확대	○ 기술검증 및 실용화 체계 구축 ○ 양자기술 활용 범위 확대	○ 글로벌 시장 선도가능한 양자 제품 개발 ○ 양자기술 분야 글로벌 TOP 4 진입
	표준개발	○ 양자암호통신 실용화를 위한 통신 전반에 대한 표준 확보	○ 양자컴퓨팅, 센싱, 통신 등 신기술 분야 표준 선점	○ 양자정보통신 시장 확보에 필요한 표준 개발

03. 표준 R&D 대상기술 선정

표준화 대상 후보 기술

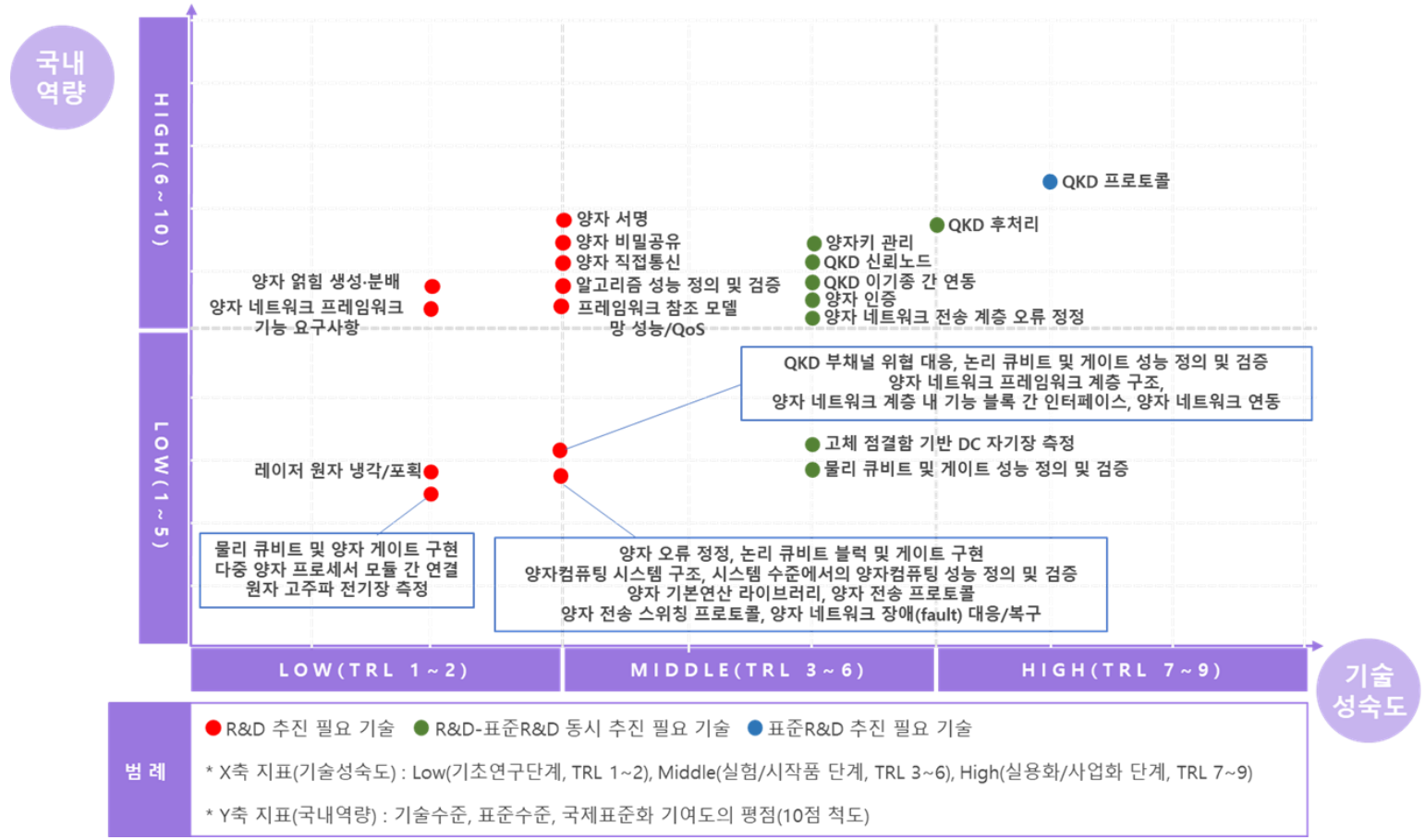
- 양자정보통신 분야 표준구조모델 개발을 통해 도출한 85개 최하위 분류체계 중 표준이 존재하지 않거나, 향후 5년 이내에 표준화 추진 가능성이 높은 기술 34개 선별

표준화 대상 후보 기술	
양자 암호통신 (10)	QKD 프로토콜
	양자인증
	양자서명
	양자 비밀공유
	양자 직접통신
	QKD 후처리 기술
	양자키 관리
	QKD 신뢰노드
	QKD 이기종 간 연동 기술
	QKD 부채널 위협 대응 기술
양자컴퓨팅 (10)	물리 큐비트 및 양자 게이트 구현
	다중 양자 프로세서 모듈 간 연결
	물리 큐비트 및 게이트 성능 정의 및 검증
	양자오류정정
	논리 큐비트 블럭 및 게이트 구현
	논리 큐비트 및 게이트 성능 정의 및 검증
	양자컴퓨팅 시스템 구조
	시스템 수준에서의 양자컴퓨팅 성능 정의 및 검증
	기본연산 라이브러리
	알고리즘 성능 정의 및 검증 기술

표준화 대상 후보 기술	
양자센싱 (3)	레이저 냉각/포획 기술
	원자 고주파 전기장 측정 기술
	고체 점결함 스핀 DC 자기장 측정 기술
양자 네트워크 (11)	양자 네트워크 프레임워크 참조 모델
	양자 네트워크 프레임워크 계층 구조
	양자 네트워크 프레임워크 기능 요구사항
	양자 얽힘 생성·분배
	양자 네트워크 전송 계층 오류 정정
	양자 전송 프로토콜
	양자 전송 스위칭 프로토콜
	양자 네트워크 장애(fault) 대응/복구 기술
	양자 네트워크 계층 내 기능 블록 간 인터페이스
	양자 네트워크 연동
	양자 네트워크망 성능/QoS

03. 표준 R&D 대상기술 선정

후보 대상 설문 결과(2023.5.8~2023.5.22)



03. 표준 R&D 대상기술 선정

표준화 대상 기술

- 기존 R&D와 중복성 여부, 국제표준화 NP 체택 가능성 등을 고려하여 11개 기술 선정

표준화 대상 기술		세부 표준화 기술	비고
양자 암호 통신	QKD 프로토콜	연속변수 및 분리변수, 준비 및 측정, 측정장치독립(MDI), 양자얽힘기반(EB) 양자키분배 규격	표준 R&D 추진
	양자 인증	양자인터넷 또는 양자네트워크 환경에서 양자얽힘 또는 단일광자를 이용한 양자인증 프로토콜	R&D-표준 R&D 동시 추진
	QKD 후처리 기술	QKD 에러 정정, 비밀증폭 등 후처리 관련 프로토콜, QKD 후처리 규격 요구사항 또는 가이드라인	R&D-표준 R&D 동시 추진
	QKD 이기종 간 연동 기술	이기종 QKD 장비 및 네트워크 연동 기술 - 양자암호장비와 제어 플랫폼 간 서비스 연동 및 품질관리를 위한 제어/운용 등	R&D-표준 R&D 동시 추진
	QKD 부채널 위협 대응 기술	QKD 부채널 공격에 대한 대응 기술, 안전성 요구사항 또는 가이드라인	R&D 추진
양자 컴퓨팅	물리 큐비트 및 게이트 성능 정의 및 검증	결맞음 유지 시간 등 물리 큐비트 성능/ 게이트 동작 정확도, 게이트 동작 시간 등 물리 게이트 / 물리 큐비트 및 게이트 성능 평가 프로토콜 또는 가이드라인	R&D-표준 R&D 동시 추진
	논리 큐비트 및 게이트 성능 정의 및 검증	논리 큐비트 및 게이트 요구사항 정의, 논리 큐비트/게이트 성능 지표 및 평가 프로토콜	R&D-표준 R&D 동시 추진
	양자 알고리즘 성능 정의 및 검증 기술	양자 알고리즘에 대한 성능 정의 및 평가 검증 기술	R&D 추진
양자 센싱	고체 점결함 기반 DC 자기장 측정 기술	단일/앙상블 점결함 센서 레퍼런스 개발 및 감도/공간해상도 시험 평가 방법	R&D-표준 R&D 동시 추진
양자 네트 워크	양자 네트워크 프레임워크 참조 모델	양자 네트워크 상세 기술규격 관련 표준화 이전 선행 참조 모델 기술 - 양자 네트워크 계층구조 참조 모델, 양자 네트워크 유즈케이스 및 서비스 시나리오	R&D 추진
	양자 네트워크 전송 계층 오류 정정	얽힘쌍 생성 및 전송에서 발생하는 잡음 감소 프로토콜 양자 네트워크를 통해 전달되는 양자상태의 손실 및 오류 보정 프로토콜	R&D-표준 R&D 동시 추진

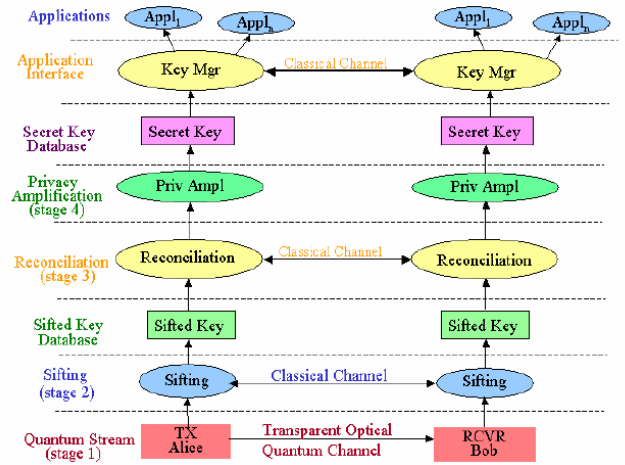
04. 표준화 대상 기술 R&D 로드맵

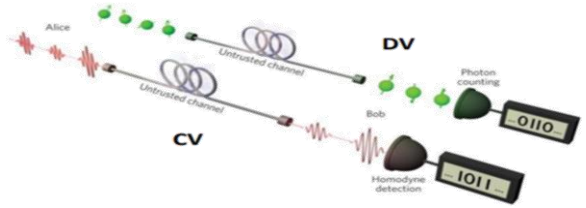
QKD 프로토콜 기술 개발

- **(기술 개발내용)**
  - QKD 프로토콜의 종류가 다양하여 현재 업계에서 표준화 작업 없이 널리 쓰이는 프로토콜의 공통 기능에 대한 의견 정립과 신규 프로토콜 성능 관련 연구 개발 동시 추진
- **(표준 필요성)**
  - QKD 프로토콜은 학계와 업계에서 30여년 넘게 사용되어 왔으나 표준화 작업없이 사용됨으로써 장비 인증 및 표준화된 프로세스 정립에 어려움 존재
- **(표준 개발내용)**
  - QKD 프로토콜 프레임워크(공통사항) 표준 및 QKD 프로토콜 그룹별 세부 요구사항 표준
  - 연속변수 및 분리변수 양자키분배 규격 / 준비 및 측정(P&M), 측정장치독립(MDI), 양자얽힘 기반(EB) 양자키분배 규격

구분		2023	2024	2025	2026	2027	2028
QKD 프로토콜	기술	◑ QKD 프로토콜 공통 요소 정립					
			○ 신규 QKD프로토콜 개발 및 기존 프로토콜 성능 개선				
	표준		● QKD 프로토콜 공통 요소 표준				
					● QKD프로토콜 종류 및 세부 표준		

< 기술 개념도 >





* 출처 : An Application of Quantum Networks for Secure Video Surveillance 2011, Nature Photonics No. 7, pp 350–352 (2013)

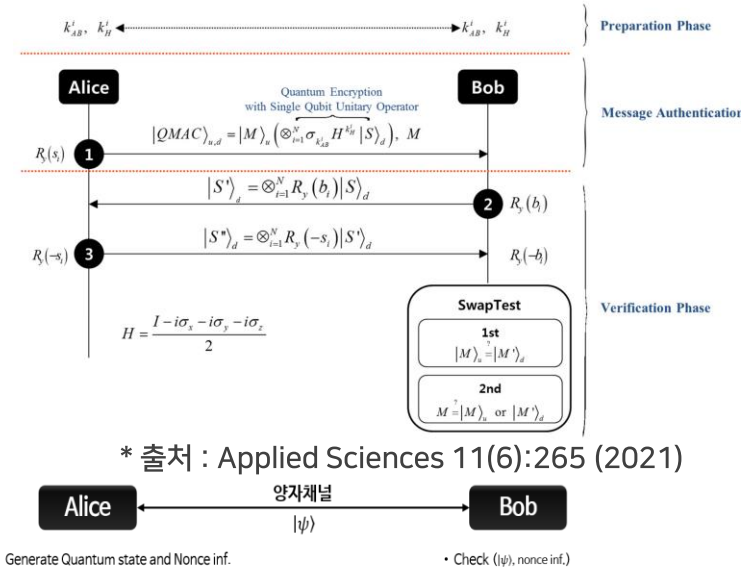
04. 표준화 대상 기술 R&D 로드맵

양자인증 기술 개발

- **(기술 개발내용)**
  - 양자 인터넷에 활용 가능한 상용 수준의 양자인증 개발 추진
  - 실망 구현이 가능한 수준 이상의 단일 광자, 얽힘 광원을 이용한 양자인증 연구개발 및 구현
- **(표준 필요성)**
  - QKD가 상용화된 현재까지도 양자 인터넷 시대에 필수 요소로 사용될 양자인증 프로토콜 및 관련 요소기술 표준 부재
- **(표준 개발내용)**
  - 양자얽힘 또는 단일광자를 이용한 양자인증 프로토콜, 양자 인터넷 또는 양자 네트워크 환경에서의 양자인증 프로토콜
  - JTC1 SC27, ETSI ISG QKD, ITU-T SG17에서 표준화 추진

구분		2023	2024	2025	2026	2027	2028
양자 인증	기술	○ 단일 광자를 이용한 양자인증 프로토콜					
			○ 얽힘 광원을 이용한 양자인증 프로토콜				
				○ 양자인증 구현/검증 기술			
	표준		● 양자인증 프로토콜 표준				
					● 양자인증 구현 표준		

< 기술 개념도 >



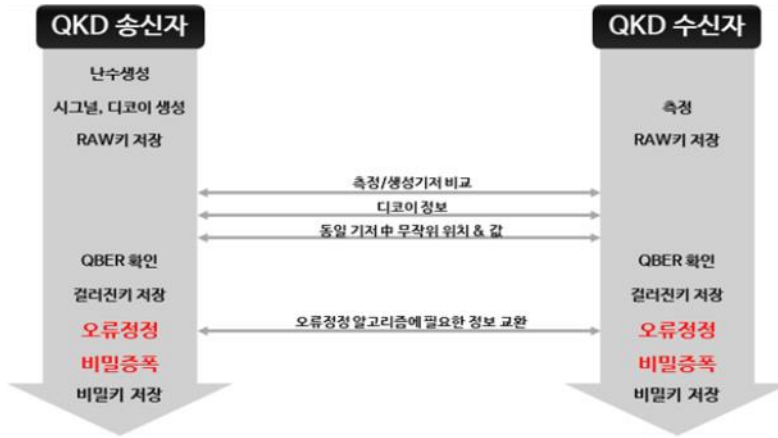
* 출처 : Applied Sciences 11(6):265 (2021)

04. 표준화 대상 기술 R&D 로드맵

QKD 후처리 기술 연구 개발

- **(기술 개발내용)**
  - 양자 인터넷을 구성하는데 기반이 되는 QKD 장비 간, 혹은 QKD 제품군과의 연동을 위한 효율적이며 안전성을 보장할 수 있는 QKD 후처리 기술 프로토콜, 최적화 연구 등의 개발
- **(표준 필요성)**
  - QKD 상용 장비마다 QKD 후처리 기술과 규격이 달라 장비 간 연동 및 QKD 장비와 통신하는 제품군의 연동이 어려움
  - QKD 장비에 대한 안전성 평가 시, QKD 후처리와 관련된 프로토콜 및 규격 표준 필요
- **(표준 개발내용)**
  - QKD 기술별 후처리 안전성 고려사항 및 이에 적합한 규격 개발
  - JTC1 SC27, ETSI ISG QKD, ITU-T SG17에서 표준화 추진

< 기술 개념도 >



구분		2023	2024	2025	2026	2027	2028
QKD 후처리 기술	기술	◑ QKD 후처리 프로토콜					
			◑ QKD 프로토콜별 후처리 최적화				
	표준		● QKD 후처리 규격 표준				
				● QKD 후처리 안전성 검증 관련 표준			

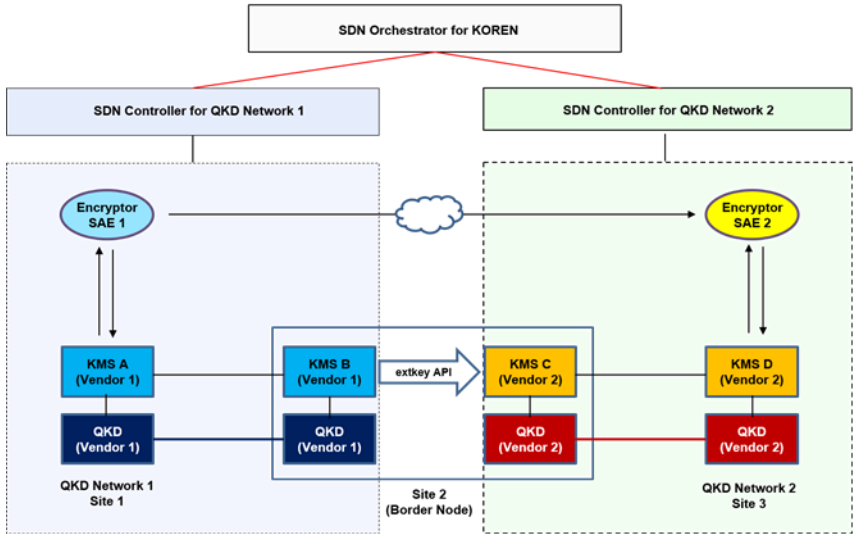
04. 표준화 대상 기술 R&D 로드맵

이기종 QKD장비 연동을 위한 키관리, 제어/운용 및 플랫폼 기술 개발

- **(기술 개발내용)**
  - 이기종 QKD 장비 연동을 위한 제어/운용 기술과 플랫폼 기술 개발 필요
  - SDN기반의 YANG모델과 이를 실제 운용망에 적용시험 하여 연동 기술 활성화 필요
- **(표준 필요성)**
  - 제조사나 통신사, 국가가 다를 경우 양자암호통신망 연결이 불가능하여 이를 QKD 기술의 단점으로 존재
  - 서로 다른 벤더의 QKD장비를 연동하여 다양한 벤더의 QKD장비를 설치하고 운용하기 위한 표준 필요
- **(표준 개발내용)**
  - ETSI ISG-QKD에서 다양한 장비 제조사 간 QKD 장비 연동을 위한 SDN기반의 YANG 모델과 관련 표준 제정

구분		2023	2024	2025	2026	2027	2028
QKD 이기종 간 연동 기술	기술	◑ 이기종 QKD 장비 연동 제어/운용 기술(SDN, YANG모델 등)					
				◑ 이기종 QKD 사업자 연동 제어/운용 플랫폼			
	표준		● 이기종 QKD 장비 연동 제어/운용 표준				
					● 이기종 QKD 사업자 연동 제어/운용 표준		

< 기술 개념도 >



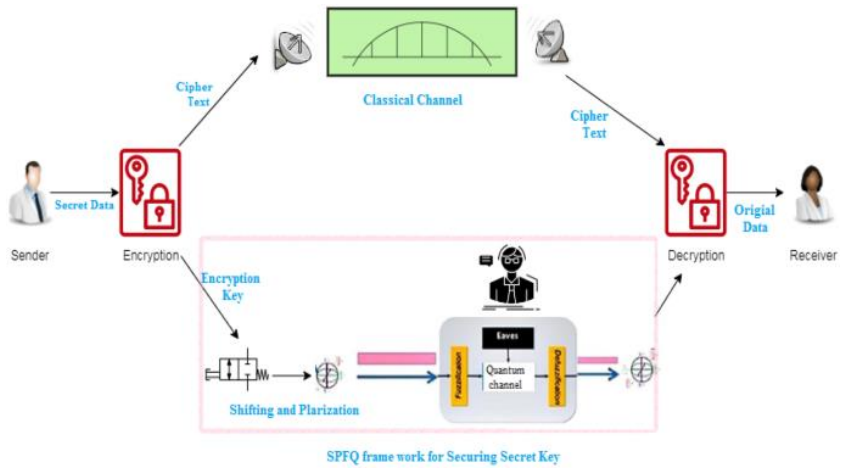
* 출처 : Entropy 2023, 25(6), 943

04. 표준화 대상 기술 R&D 로드맵

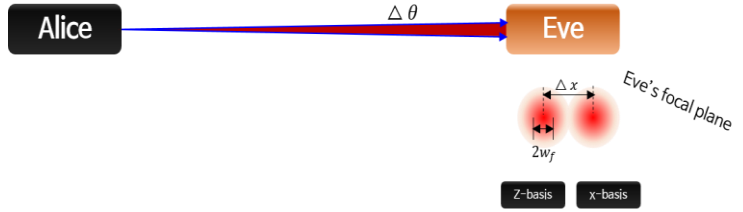
QKD 장비의 부채널 공격에 대한 안전성을 보장하기 위한 부채널 위협 대응 기술 개발

- **(기술 개발내용)**
  - 완벽하지 못한 부품들로 구현될 수 밖에 없는 QKD장비에서 부채널 공격 발생 가능
  - 다양한 유선/무선 QKD 기술별 부채널 공격 도출 및 대응 기술 개발
- **(표준 필요성)**
  - 안전한 QKD 장비개발을 지원하고 안전성 검증을 위한 부채널 위협 대응기술 표준 필요
- **(표준 개발내용)**
  - QKD 부채널 공격에 대한 대응 기술, QKD 부채널 공격에 대한 안전성 요구사항 또는 가이드라인
  - JTC1 SC27, ETSI ISG QKD, ITU-T SG17에서 표준화추진

< 기술 개념도 >



* 출처 : Brazilian Journal of Physics volume 53, Article number: 35 (2023)



구분		2023	2024	2025	2026	2027	2028
QKD 부채널 위협 대응 기술	기술	○ QKD 기술별 부채널 공격 및 대응 기술개발					
	표준		● QKD 부채널 공격 및 대응 기술 표준				
				● QKD 부채널 공격에 대한 안전성 /시험 요구사항 표준			

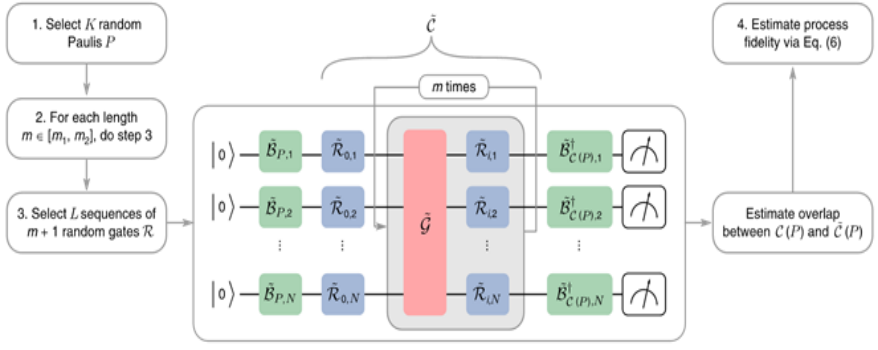
04. 표준화 대상 기술 R&D 로드맵

고성능 양자컴퓨팅 HW 개발을 위한 물리 큐비트 및 게이트 성능 분석 기술 개발

- **(기술 개발내용)**
  - 양자회로 단위의 성능을 정의하고 정확하고 효율적으로 평가하며 다중 큐비트 결맞음 시간 측정 기술 개발 필요
  - HW 기술 성능 평가와 소프트웨어적인 전/후처리 프로세스를 추가 적용을 통해 확보 가능한 성능을 구분할 수 있는 양자회로 동작 정확성 검증 및 성능평가 기술 개발
- **(표준 필요성)**
  - 양자컴퓨팅 HW에 대한 서로 상이한 방식에 의한 성능평가 결과들이, 추후 양자컴퓨팅 산업화 단계에서는 신뢰성의 문제를 야기할 수 있음
- **(표준 개발내용)**
  - 큐비트 결맞음 시간, 양자 게이트 동작 정확성 검증 방법 및 양자회로 성능 평가에 관한 표준

구분		2023	2024	2025	2026	2027	2028
물리 큐비트 및 게이트 성능 정의 및 검증	기술	◑ 다중 큐비트 결맞춤 시간 측정 기술					
			◑ 양자 게이트 동작 정확성 검증 효율성 향상 기술				
				◑ 양자회로 동작 정확성 분석 기술			
	표준	● 큐비트 결맞음 시간에 관한 표준					
			● 양자 게이트 동작 정확성 검증 방법에 관한 표준				

< 기술 개념도 >



양자회로 벤치마크 회로

* 출처: nature comm. 10, 5347 (2019)

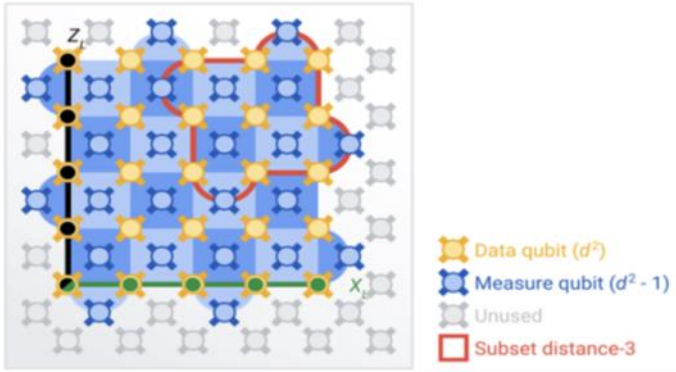
04. 표준화 대상 기술 R&D 로드맵

결함허용 양자컴퓨팅 구현 및 성능 고도화를 위한 논리 큐비트 및 게이트 성능 검증 기술 개발

- **(기술 개발내용)**
  - 오류정정 및 결함허용 양자컴퓨팅 기술에 대한 개발도 본격화되고 있어 오류정정이 적용된 논리 큐비트 및 게이트에 대한 정확한 요구조건 및 성능 분석 기술 개발
- **(표준 필요성)**
  - 결함허용 양자컴퓨팅 구현에 필요한 HW의 요구조건과 양자컴퓨팅 구동 시간 및 정확도에도 차이가 발생하게 되므로, 결함허용 양자컴퓨팅 구현을 위한 요구조건과 논리적 큐비트 및 게이트의 성능에 대한 지표 및 평가방법의 표준 필요
- **(표준 개발내용)**
  - JTC1, IEEE 등 양자컴퓨팅 HW 기술 개발 기관과 표준화 전문 전문가 간 협업 체계를 구축을 통한 양자 오류 임계값 및 논리 큐비트 성능 관련 표준 개발

구분		2023	2024	2025	2026	2027	2028
논리 큐비트 및 게이트 성능 정의 및 검증	기술	○ 실용적인 양자 오류 임계값 분석 기술					
				○ 논리 큐비트 구현에 따른 비용 및 성능 분석 기술			
	표준	● 양자 오류 임계값에 대한 표준					
				● 논리 큐비트 성능에 관한 표준			

< 기술 개념도 >



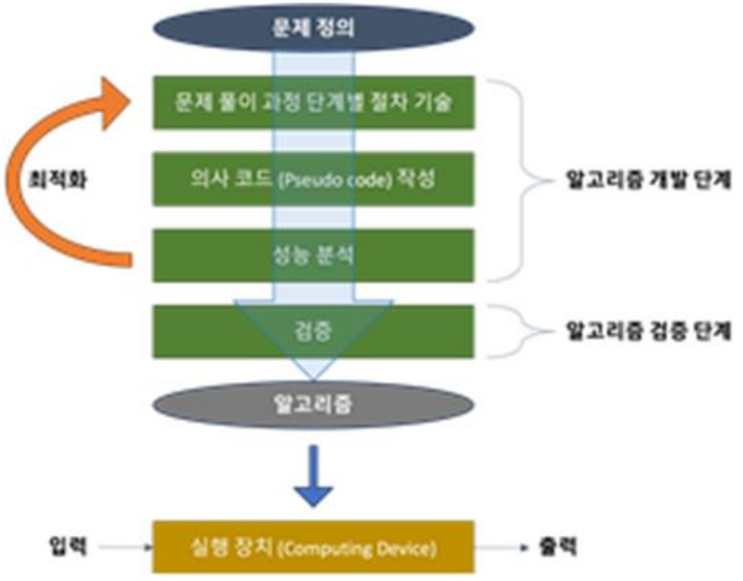
* 출처: 구글 AI 퀀텀 블로그

04. 표준화 대상 기술 R&D 로드맵

양자컴퓨팅 활용성 향상을 위한 양자 알고리즘 성능 검증 기술개발

- **(기술 개발내용)**
  - 고전 알고리즘 대비 양자 알고리즘의 우월성을 엄격하게 평가할 수 있는 분석 기술 연구개발
  - 복잡도 분석에 머무르지 않고, 실제 알고리즘 구동 관점에서 양자 알고리즘 우월함을 검증할 수 있는 기술 개발
- **(표준 필요성)**
  - 자원량 중심의 복잡도 분석에서 벗어나 실행관점에서 성능 측정을 위한 표준 부재
- **(표준 개발내용)**
  - JTC1, IEEE 등 양자컴퓨팅 알고리즘 기술 개발 기관과 표준화 전문 전문가간 협업 체계를 통해 양자 알고리즘 우월성, 구동 요구자원량 평가, 구동 예산 성능 평가 표준 개발

< 기술 개념도 >



구분		2023	2024	2025	2026	2027	2028
양자 알고리즘 성능 정의 및 검증 기술	기술	○ 양자 알고리즘의 우월성 판단 기술					
		○ 양자 알고리즘 구동 요구 자원량 분석 기술					
				○ 양자 알고리즘 구동 예상 성능 평가 기술			
	표준	○ 양자 알고리즘 우월성 관련 표준					
		○ 양자 알고리즘 구동 요구 자원량 평가 표준					
				○ 양자 알고리즘 구동 예상 성능 평가 표준			

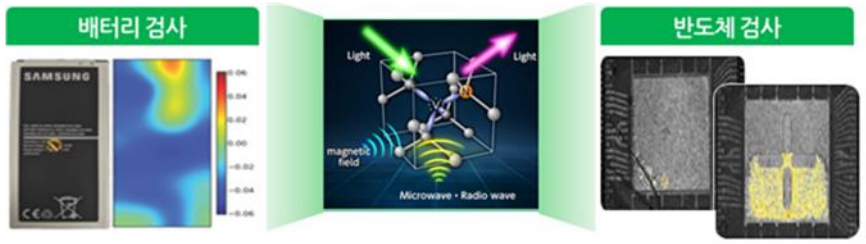
04. 표준화 대상 기술 R&D 로드맵

양자 자기장센서 응용분야 확대를 위한 센서 성능 시험평가 기술개발

- **(기술 개발내용)**
  - 감도 및 공간해상도 측정을 위한 레퍼런스 센서(단일 점결함/앙상블 점결함 자기장 센서)의 개발과 시험평가 방법 관련 기술 개발
- **(표준 필요성)**
  - 레퍼런스 센서를 기준으로 공신력있는 센서의 스펙을 평가할 수 있는 시험평가 표준이 선행되어야 다양한 응용분야의 자기센서 수요자들이 용도에 맞게 폭넓게 활용
- **(표준 개발내용)**
  - TTA 양자정보통신 PG 신설을 통해 고체 점결함 자기장 센서의 감도 및 공간해상도를 평가할 수 있는 시험평가 표준화 추진 필요

구분		2023	2024	2025	2026	2027	2028
고체 점결함 기반 DC 자기장 측정 기술	기술	○ 단일 점결함 레퍼런스 자기센서 기술					
		○ 양상블 점결함 레퍼런스 자기센서 기술					
	표준			◑ 단일 점결합 자기센서 시험평가 표준			
				◑ 앙상블 점결합 자기센서 시험평가 표준			

< 기술 개념도 >



* 출처: 양자정보기술백서 2022

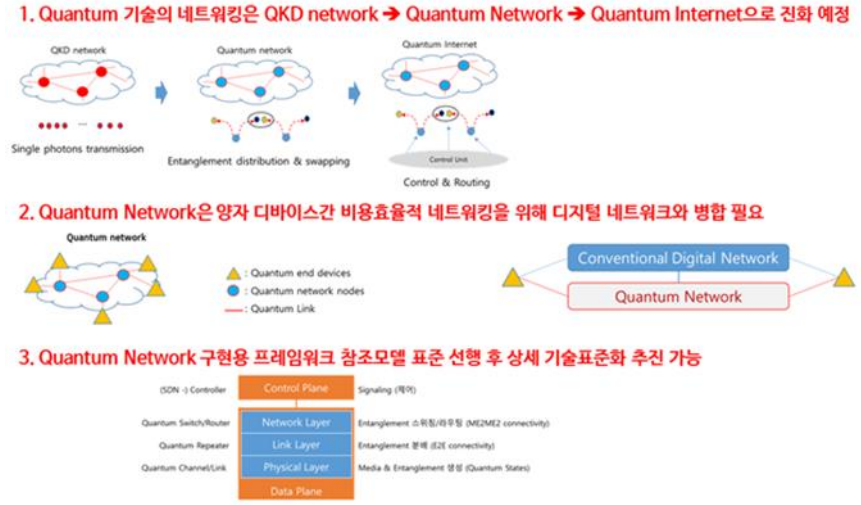
04. 표준화 대상 기술 R&D 로드맵

양자 네트워크 표준화 선점을 위한 양자네트워크 프레임워크 기술 개발

- **(기술 개발내용)**
  - 양자 네트워크 상세 기술규격 관련 표준화 이전 선행 참조 모델 기술
  - 양자 네트워크 계층구조 참조 모델, 양자 네트워크 유즈케이스 및 서비스 시나리오
- **(표준 필요성)**
  - 양자네트워크 계층구조, 계층별 기능, 서비스 기술 등과 관련한 한국에 유리한 혹은 차별적인 기술 개발 방향 도출
- **(표준 개발내용)**
  - ITU-T SG11, SG13 등에서 계층구조와 기능, 서비스 등의 참조모델 관련 국제표준 선점과 함께 물리 혹은 링크 계층에 해당하는 양자 오류 정정 기술에 대한 표준화도 선점 병행 추진

구분		2023	2024	2025	2026	2027	2028
양자네트워크 프레임워크 참조 모델	기술	○ 양자네트워크 계층구조 기술					
			○ 양자네트워크 계층별 기능				
				○ 양자네트워크 서비스 기술			
	표준		○ 양자네트워크 계층구조 표준				
				○ 양자네트워크 요구사항 표준			
					○ 양자네트워크 시나리오 표준		

< 기술 개념도 >



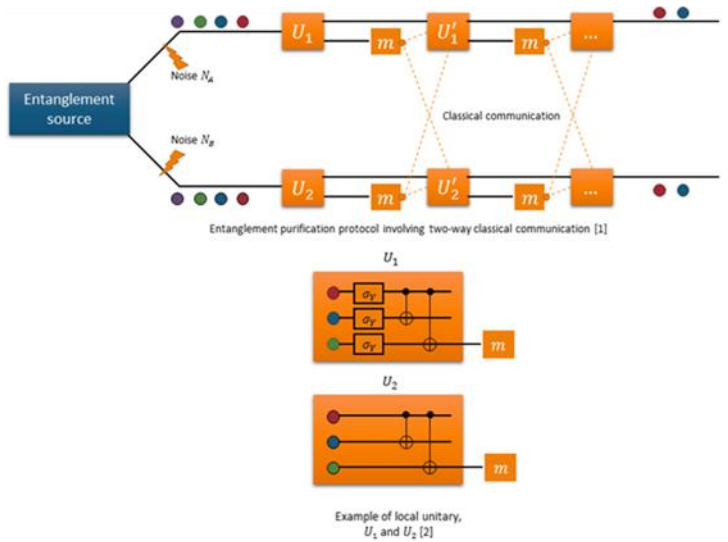
04. 표준화 대상 기술 R&D 로드맵

양자 얽힘 생성 및 전송을 위한 얽힘 정제 및 손실 보정 기술개발

- **(기술 개발내용)**
  - 얽힘쌍 생성 및 전송에서 발생하는 잡음 감소 프로토콜
  - 양자 네트워크를 통해 전달되는 양자상태의 손실 및 오류 보정 프로토콜
- **(표준 필요성)**
  - 다양한 형태의 양자상태 오류정정 기술이 존재하나 양자네트워크 구성을 위한 보안 기준(얽힘 정제, 성능지표, 손실보정 등) 및 디지털 인터넷 보안 계층과의 융합 범위 정의 필요
- **(표준 개발내용)**
  - ITU-T SG13에서 양자네트워크 계층별 역할 정의 및 디지털 인터넷과 인터페이스 표준 개발

구분		2023	2024	2025	2026	2027	2028
양자네트워크 전송계층 오류 정정	기술	◑ 얽힘 정제 기법					
		◑ 양자 전송 손실 보정 기법					
	표준			● 얽힘정제 기법 및 성능지표 표준			
					● 양자 전송 손실 보정 기법 표준		

< 기술 개념도 >



* 출처: Physical review letters 76.5 (1996): 722

감사합니다.

권대성 연구위원, ETRI 부설연구소
cryptkwon@gmail.com