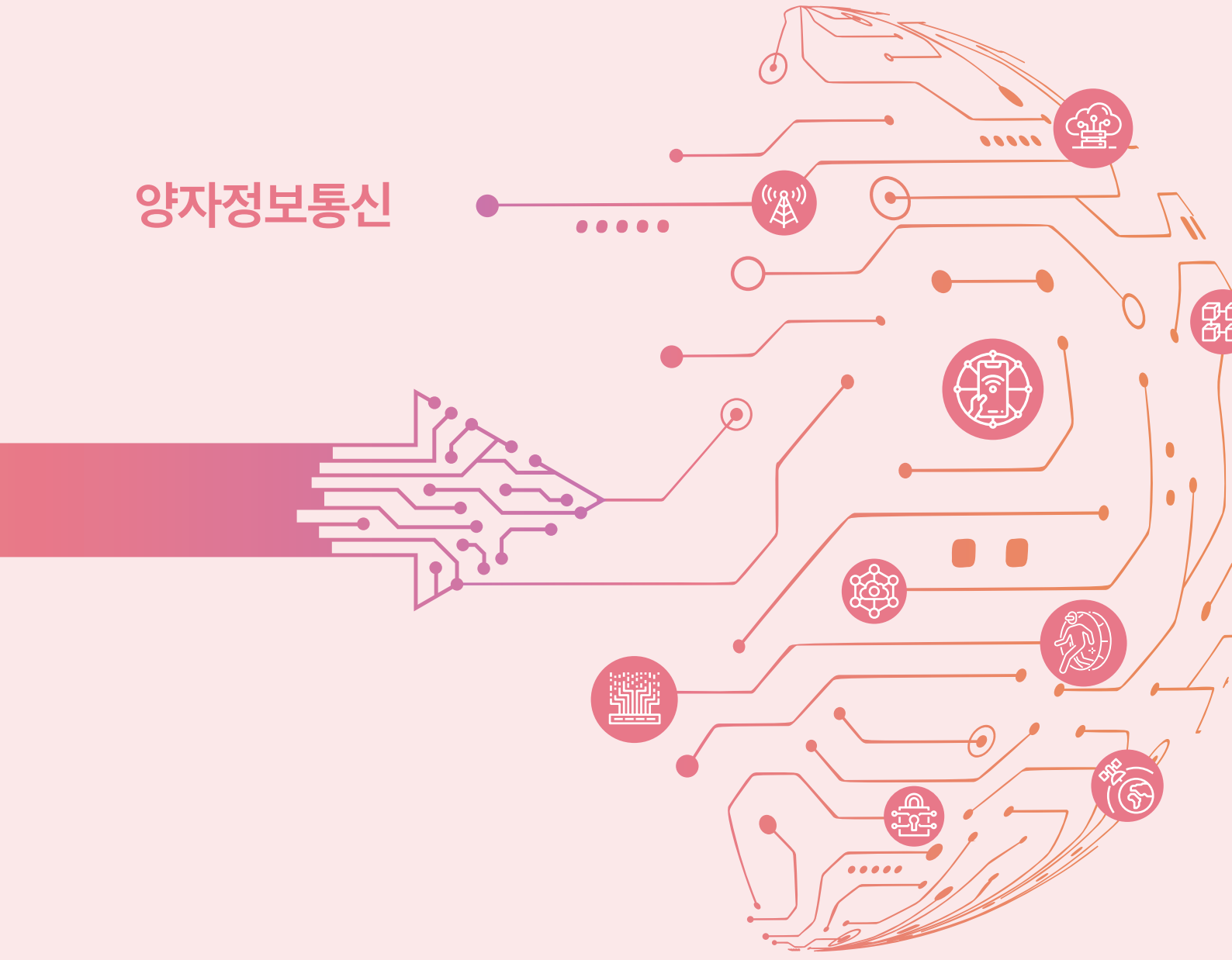
Ver. 2023

ICT 표준화 전략맵

ICT Standardization Strategy Map

양자정보통신



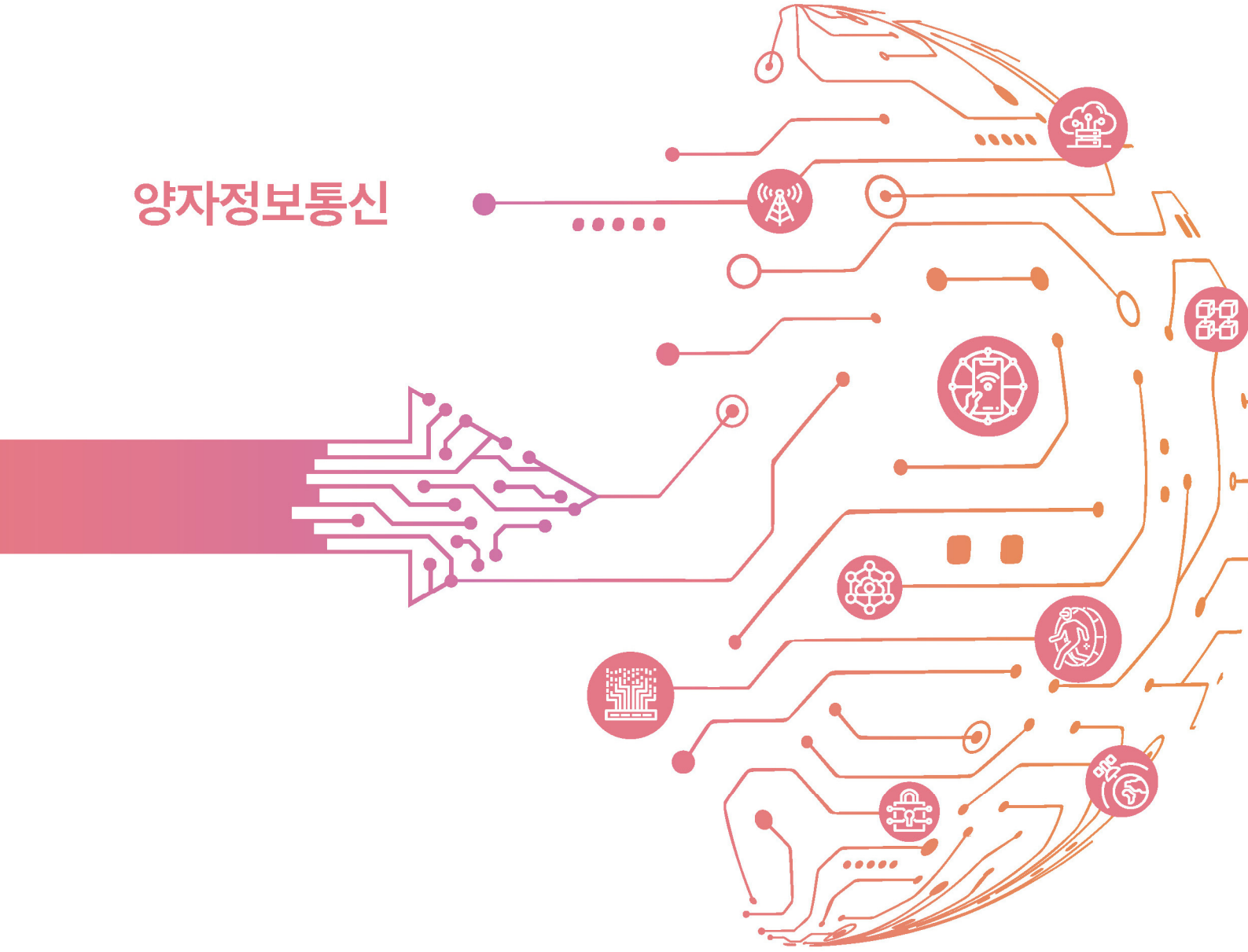
TTA 한국정보통신기술협회
Telecommunications Technology Association

Ver. 2023

ICT 표준화 전략맵

ICT Standardization Strategy Map

양자정보통신



Ver. 2023

ICT Standardization Strategy Map

ICT 표준화 전략맵

Contents

양자정보통신

ICT Standardization Strategy Map

Part

I

표준화 개요

Ⅰ. 표준화 개요

1.1. 기술 개요

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 구성하였다.

o (양자암호통신) 송신자와 수신자 사이에 단일광자 또는 공유된 얽힘(entanglement) 상태의 비가역성, 불확정성 원리를 활용하여 암호키분배, 서명, 인증 등 암호기능을 구현하는 기술

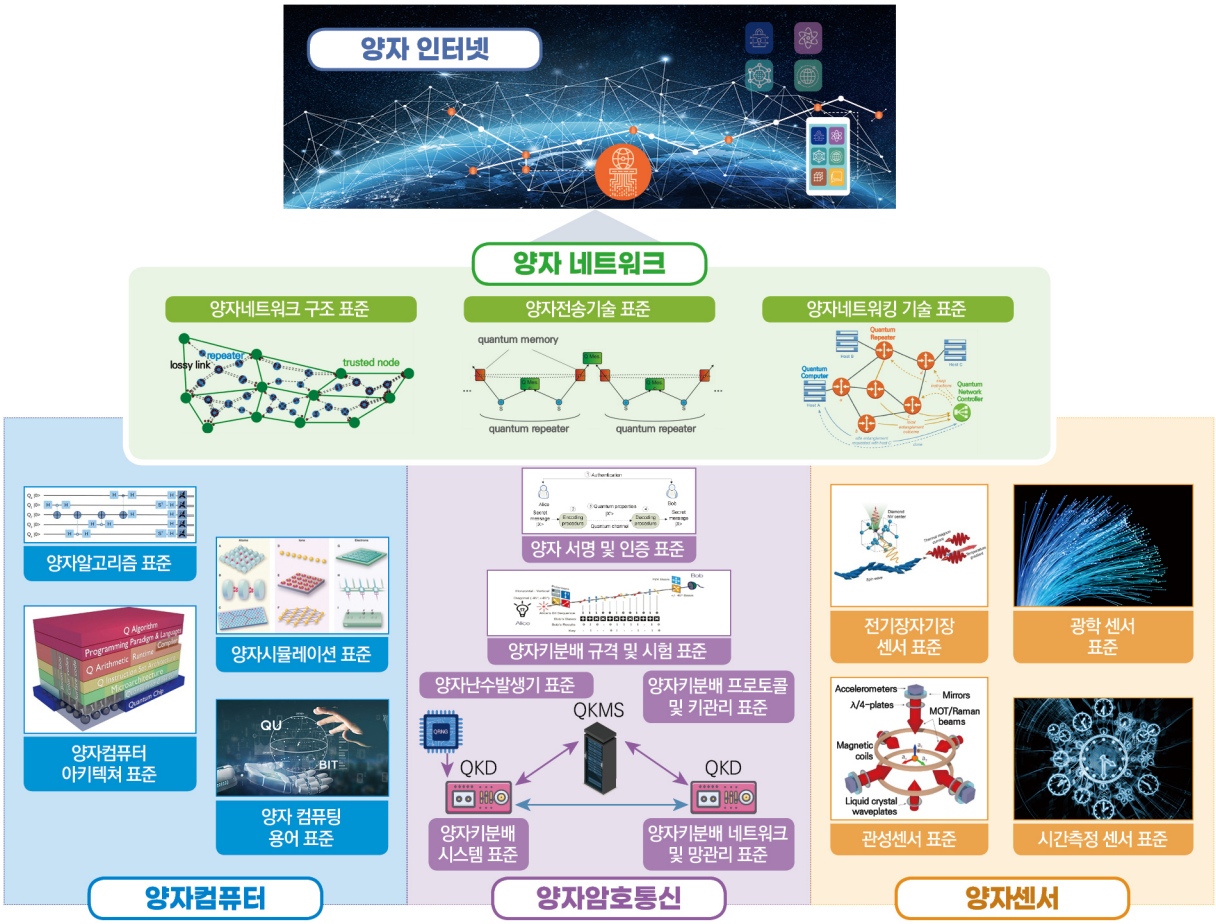
o (양자 컴퓨팅) 양자역학을 정보처리에 적극적으로 활용하는 컴퓨팅 기술로, 중첩(superposition) 및 얽힘 등의 양자역학 고유의 현상들을 기반으로, 특정 연산들에 대해 기존 디지털 컴퓨팅으로는 현실적인 시간 안에 불가능했던 계산을 가능하게 하는 기술

o (양자 센싱) 입자로서의 특성과 파동으로서의 특성을 모두 나타내는 낱개의 원자와 같은 개별 양자 개체(individual quantum object)를 센서로 사용하거나, 입자 사이의 얽힘이나 불확정성의 압착(squeezing) 현상과 같은 비고전적인 양자 원리를 활용함으로써 고전 시스템을 사용한 센싱·계측 기술의 분해능, 민감도와 측정영역의 한계를 극복하는 기술

o (양자 네트워크) 두 개 이상의 양자기기(양자컴퓨터, 양자센서, 양자키분배 장치 등) 간에 양자 정보(광자 혹은 원자상태)를 안전하고 효율적으로 전달하는 네트워크 기술

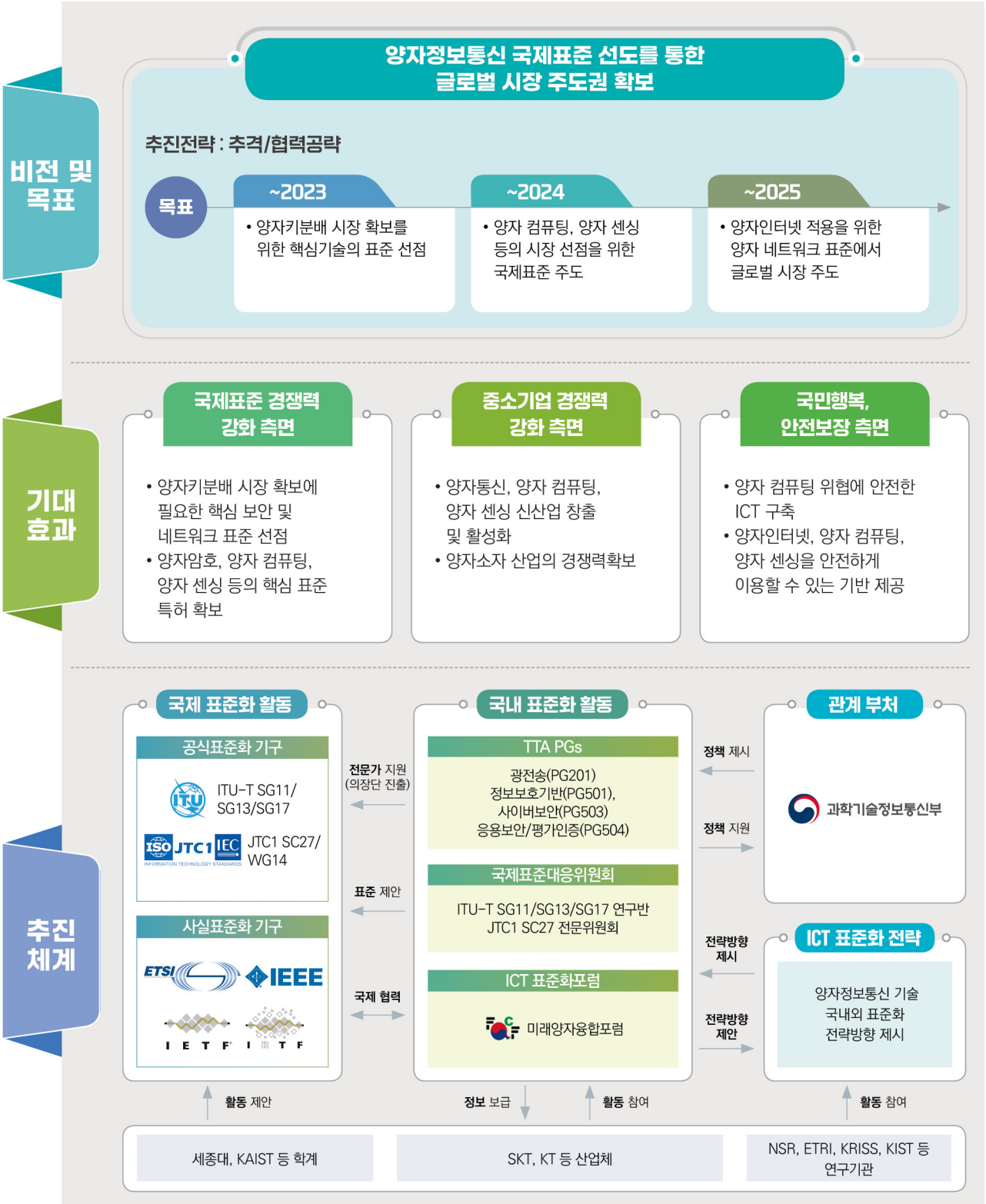
o (양자 인터넷) 양자 네트워크를 이용하여 다양한 디바이스 연결 및 서비스를 제공하는 인터넷을 구현하는 기술로, 양자정보통신 관련 요소 기술 개발이 중심이 되는 현재 상황을 고려하여 이번 ICT 표준화 전략(Ver.2023)에서는 포함하지 않음

< 양자정보통신 분야 개념도>



1.2. 표준화 비전 및 기대효과

o 표준화 비전



o 비전 및 목표

- 추진전략

  • 양자정보통신 기술은 기존 정보통신의 한계를 극복할 수 있는 기술로, 세계적으로 기술개발이 활발히 이루어지고 있으나 실용화에 근접한 양자키분배를 제외하고는 표준 개발이 초기 단계로, 양자 컴퓨팅, 양자 센싱 등 기술 전반에서 기술개발 선진국과의 다각화된 협력을 통한 주도권 확보가 필요하여 '추격/협력공략'으로 선정

< 표준화 목표 >

구분	주요내용
~ 2023년	- 양자키분배 시장 확보를 위한 핵심기술의 표준 선점 • ITU-T SG13/SG17 등 양자키분배 관련 국제표준화 기구에서 다양한 적용 관련 표준 선점 추진
~ 2024년	- 양자 컴퓨팅, 양자 센싱 등의 시장 선점을 위한 국제표준 주도 • 표준 초기 단계이지만 새로운 시장 창출력이 큰 양자컴퓨팅, 양자 센싱 분야에서의 기술 확보와 더불어 활용 관련 표준 선점 추진
~ 2025년	- 양자 인터넷 적용을 위한 양자 네트워크 표준에서 글로벌 시장 주도 • 양자컴퓨터 간, 양자 센싱 정보 교환, 자체 보안기술 등에 대하여 표준 선점 추진

o 표준화 기대효과

- 국제표준 경쟁력 강화 측면

  • 국내의 시범사업 경험을 기반으로 양자키분배 시장 확보에 필요한 핵심 보안 및 네트워크 표준 선점

  • 기술개발 단계인 양자 암호, 양자 컴퓨팅, 양자 센싱 등의 활용을 고려한 핵심 표준 특허 확보

- 중소기업 경쟁력 강화 측면

  • 양자통신, 양자 컴퓨팅, 양자 센싱을 다양한 기기 및 서비스에 적용한 新산업 창출 및 활성화

  • 양자정보통신 개발에 필요한 다양한 양자 소자의 자제 공급망 확보에 필요한 소자 산업의 경쟁력 확보

- 국민행복·안전보장 측면
  - 현 인터넷에 대한 양자 컴퓨팅 위협을 제거할 수 있는 양자 인터넷 구축 및 다양한 국민안심 서비스 제공
  - 양자 인터넷, 양자 컴퓨팅, 양자 센싱 등을 다양한 분야에 안전하게 활용할 수 있는 기반 제공

양자정보통신

ICT Standardization Strategy Map

Part

II

국내외 현황분석

2.1. 정책 현황 및 전망
2.2. 기술개발 현황 및 전망
2.3. IPR 현황 및 전망
2.4. 표준화 현황 및 전망

Ⅱ. 국내외 현황분석

2.1. 정책 현황 및 전망

구분	주요 현황
한국	- 과기정통부, '대한민국 디지털 전략' 발표를 통한 6대 디지털 혁신기술 분야의 연구개발 집중 투자 추진('22.9) ① 인공지능, ② 인공지능 반도체, ③ 5G·6G 이동통신 ④ 양자, ⑤ 확장가상세계, ⑥ 사이버보안 - 윤석열 정부, 120대 국정과제 발표(2022.7.) • 과학기술 5대 강국 도약을 위한 필수적 전략기술 지정 • ①반도체·디스플레이, ②이차전지, ③차세대 원전, ④수소, ⑤5G·6G, ⑥바이오, ⑦우주·항공, ⑧양자, ⑨AI·로봇, ⑩사이버보안 - 국정원, 양자암호통신 시험검증제도 시행(2022.6.) • 세계 최초로 QKD 장비를 국가 공공분야에 도입하기 위한 보안 적합성 검증기준 마련 • 시험기관을 TTA, ETRI, 인증사무국 등을 지정하여 2023년도에 본격 시행 - 과기정통부, 양자기술 집중 육성 사업 계획(2022.1) • 핵심원천기술 개발과 인력양성, 기술 사업화에 814억원 투자 계획 (2021년 투자 대비 67% 증가) - 과기정통부, 양자 등 10개의 국가 필수전략기술 선정 발표(2021.12) • ①인공지능, ②5G,6G, ③첨단바이오, ④반도체·디스플레이, ⑤이차전지, ⑥수소, ⑦첨단로봇·제조, ⑧양자, ⑨우주·항공, ⑩사이버보안 • 초고속 연산·초정밀 계측 등 현재 컴퓨팅 기술 한계를 뛰어넘어 신약개발, 금융 등 다양한 산업에서 양자 혁명을 초래할 것으로 전망 • 미·중·일·유럽연합 등 모든 주요국의 공통 전략기술로, 국가 차원 전폭적 지원 • 보안 강화(양자암호통신)와 암호체계 무력화(양자컴퓨팅)라는 양면성으로 국가안보 관점에서도 매우 큰 전략적 가치를 지닌 기술 - 과기정통부, 과학기술 관계 장관회의에서 '양자기술 연구개발 투자전략' 수립(2021.4) • 한국연구재단 및 정보통신기획평가원에서 국가 R&D 진행(1천 520억원) • 산·학·연, 국가 차원의 중장기 비전과 투자전략을 마련 • 목표: 2030년대 양자 기술 4대 강국 진입 - 과기부와 한국지능정보사회진흥원(NIA), '양자암호통신 인프라 시범 사업'(2020.12) • KT, SKB, LGU+와 중소기업 컨소시엄 총 18개 공공·의료·민간기관을 대상으로 양자 인프라 구축과 시험 검증 진행 • 양자기술 사업화 및 실증을 위한 양자센서(중력, 자기장) 개발 과제 진행(2022.07, 1.5년) - 과기부, 양자컴퓨팅, 양자통신, 양자센서, 양자인터넷 및 양자정보과학 생태계 조성사업 발표(2019.3) • 양자정보과학 기술의 독자적 기술 확보 목적 • 양자 컴퓨팅 연구인프라 구축 사업(2022~2026, 490억) 및 양자인터넷 핵심원천기술개발 사업(2022~2026, 456억) 출범 • 2019년 시작되어 2022년 종료하는 양자센서 핵심원천기술개발 사업에 연계된 후속 브릿지 사업 기획(2023년 착수 예정)

구분	주요 현황
미국	- 백악관, 양자정보과학 우위 확보를 위한 양자정보과학(QIS) 관련 지침 2건 발표(2022.05) • 양자정보과학과 기술 응용분야에서 미국의 주도권이 계속되도록 조치하기 위한 행정명령 • 양자정보과학에서 미국의 경쟁 우위를 유지하고, 미국의 사이버, 경제, 국가 안보에 미치는 양자 컴퓨터의 위험을 완화하는 데 필요한 핵심 조치를 포함한 국가안보 공문 - 백악관, '국가 양자 이니셔티브 위원회' 신설 행정명령 발표(2022.5) • 백악관 과학기술정책(OSTP) 실장, 산업계, 대학 및 연방 정부 대표로 구성되며, 미 에너지부에 보고하지 않고 백악관에 직접 보고할 예정 - 미국의회, 자국의 경제 및 국가안보 강화를 위한 '미국 경쟁법(The America COMPETES Act of 2022)' 제정(2022.2) • 하원에서 양자정보과학 및 양자정보통신을 포함하는 분야의 기술·혁신 경쟁력 강화 등의 내용을 포함하는 "2022년 미국 경쟁법" 통과 - 미국의회, 양자 인터넷망 구현을 위한 '양자 인터넷법' 발의(2020.12) • 에너지부 주관, 양자 네트워크 전략 비전(2020.7) 기반 • 양자 인터넷을 미대륙에 구현하는 것을 목표 (예산 약 2,000억원) - 백악관, 국가양자조정실은 양자정보과학 연구의 8대 우선 과제를 제시하는 양자 프론티어 보고서 발표(2020.10.) • 사회에 제공하는 혜택 확대, 양자 공학 규율 마련, 소재 과학의 맞춤 개발, 양자 시뮬레이션을 통한 이해, 정밀 측정 부문에의 활용, 새로운 활용을 위한 양자 얽힘, 양자 에러의 특성화와 감소, 양자를 활용한 우주의 이해 등 제시 - 미국 국립과학재단(NSF), 5개 양자정보과학연구센터(MS, 하버드大, 코넬大, 인텔, 록히드마틴 참여)의 설립·지원(7천억원) 정책 발표(2020.8) • 양자 네트워크를 위한 전략적 비전('20.2, NQCQ), 양자인터넷 전략비전('20.7, 에너지부) • 관련 예산확보를 통해 양자인터넷, 양자정보 전송 등 기술개발 및 표준화 준비 착수 - 미국의회, 국가적 양자기술 지원을 위한 '양자연구집중지원법'(NQI Act) 제정(2018.12) • 초기 5년간 12억 달러(1조 5800억원)를 양자 연구에 투자 • 국립표준기술연구소, 국립과학재단, 에너지부 중심으로 정책 추진 • 백악관 직속 '국가양자조정실(NQCO, The National Quantum Coordination Office)' 설치 • 대통령 자문을 위한 '국가양자자문위원회' 설립
일본	- 일본 정부, 양자 미래 사회 비전 발표(2022.4) • 사회경제 시스템으로 양자 기술을 취득하고, 활용 추진 • 2030년까지 양자 기술 이용자를 1,000만명 수준으로 확대 • 양자 기술을 이용한 생산액을 40조엔(약 493조원) 규모로 육성 - 일본 정부, 양자기술 이노베이션 전략(2020.1)을 중심으로 기술개발을 위한 장기적 투자 기반 마련 및 개정(2022.01) • 기존 이노베이션 전략은 중장기적인 연구개발에 주안점(양자 중계기, 양자 컴퓨터 등) • 최근 기술패권 경쟁과 글로벌 공급망 이슈를 감안하여, 양자기술의 조기산업화, 지식재산권화·표준화, 관련 스타트업의 육성 및 양자인터넷 연구강화 등에 주력하는 방향으로 조정 - 미-일 정상회담, 바이오, 양자, 우주 기술 등에서 협력강화 발표(2021.4.) - 일본 정부, 양자기술혁신전략(量子技術イノベーション戦略) 마련(2020.1) • 양자기술을 일본이 지향하는 "Society 5.0" 및 "데이터 기반 사회"의 경쟁력 원천인 미래 필수 기반 기술로 인식

구분	주요 현황
일본	• 양자기술과 함께 기반기술(공정, 제작, 측정 등) 혁신을 추진하며, 5대 전략분야(기술개발, 국제협력, 산업혁신, 지적재산권 및 표준화, 인재)별 추진계획 제시 - "미·일 양자협력에 관한 도쿄 성명" 발표(2019.12) • 미국과의 양자기술동맹 강화 목적 - 일본 문부과학성, 「제5기 과학기술기본계획」에 양자기술을 우선순위에 포함(2016.3)
유럽	- 프랑스, 산업 및 기술주권 강화의 일환으로 양자기술 연구개발에 5년간 18억 유로를 지원하는 계획 발표(2021. 01) - EU 양자인터넷 협의체(QIA), 산·학, 정부가 모두 참여하여 '단기·중장기 양자기술 로드맵을 제시한 '전략 연구 전략(Strategic Research Agenda)'를 발표(2020.2) • QKD, QRNG 시스템 단순화 및 성능 개선, QKD, QRNG 기술 성능평가를 위한 인증 기준 설립, 소규모 양자 중계기 기술 시연 등(단기목표) • 양자 중계기 망을 이용한 800km 이상 양자통신 시연, 최소 20개 큐빗이 연결된 양자 네트워크 시연(중·장기목표) - 영국, '19년부터 5년간 2억3천5백만 파운드(3,400억원) 투자하여 새로운 국립양자컴퓨팅센터(NQCC) 설립, 양자기술 상용화 추진, 새로운 박사급 인력양성 센터 설립 추진 정책 발표(2018. 11) - EU, 유로 QCI(European Quantum Communication Infrastructure) 출범(2019.6) • 안전한 양자통신 기반시설 확보 목적 - EU, 양자 플래그십 프로젝트 착수(2018. 10) • 세부연구 분야는 ①양자 컴퓨팅, ②양자 시뮬레이션, ③ 양자 센싱·측정학, ④양자통신, ⑤기초 양자과학 등 5개 영역으로 구성 - EU, QIA(양자인터넷연합)을 결성하고 다중 양자네트워크 간 통합시험을 통해 범유럽 인터넷 기반을 마련(2018.10) • 4개 양자컴퓨터 노드를 양자 중계기(얽힘, 텔레포트)로 연결되는 다중 양자네트워크 기술 및 양자 인터넷용 SW 프로토콜 스택 개발 - 독일, 연방정부의 프레임워크 프로그램을 통해 양자컴퓨터, 양자통신, 양자기반측정기술, 양자시스템 기초기술 등 4개 분야에 2022년까지 6억5천만 유로(8,300억원) 투자(2018.9)
중국	- 중국 정부, 「14차 국가경제사회발전 5개년 계획과 2035년 비전」 수립(2021.3) • 과학기술 선도 분야 : 인공지능, 양자정보, 집적회로, 뇌과학 및 뇌모방, 유전자 및 바이오기술(생물 육종 등), 임상의학 및 건강, 심우주 및 심층지각 및 심해 및 극지 탐험의 7개 분야 - 중국정부, 「제13차 중국 5개년 계획」부터 '양자기술'을 국가 중대 프로젝트로 규정(2016.5) • 1,000억 위안 투자 (약 19조원) • 인재 양성, 중대형 프로젝트 추진
기타	- 캐나다, 국가 양자 기술 발전을 지원하기 위해 137.9 백만 달러 규모의 신규 투자 계획 발표(2022.3) - 호주, 양자 기술을 포함하는 미래 핵심기술 청사진 및 시행계획을 발표(2021.11) • 양자통신, PQC, 양자컴퓨팅, 양자센서 등 양자 기술에 1,009억원 투자계획 발표 - 이스라엘, 양자이니셔티브(INQI : Israel National Quantum Initiative)를 '19년 설립하고 '25년까지 3억2천5백만 유로의 예산 투자 계획 발표

2.2. 기술개발 현황 및 전망

구분	상대기술수준(100%)				
	한국	미국	일본	중국	유럽
기술수준	80	100	80	90	90
※ 기술 수준은 "ICT 기술 및 표준 수준 조사" 설문조사에 의한 결과 값을 활용					

2.2.1. 국내 기술개발 현황 및 전망

[양자 암호통신]

o 양자암호통신 중 QKD는 상용화에 성공한 첫 사례로, 국내의 경우 SK텔레콤과 KT를 중심으로 국내 시장을 선도하고 있음

- 양자암호통신 중 QKD 기술은 해외에 이어 국내에서도 2020년 상용화 단계에 진입함
- 현재 국내 QKD 시스템에 가장 많이 적용된 BB84 프로토콜의 거리 한계와 일부 부채널 공격의 취약성을 개선한 MDI-QKD(measurement device independent-QKD, 측정기기무관 양자키분배) 프로토콜이 연구실 수준에서 연구되고 있음
- 현재 KT와 KT의 기술이전을 받은 우리넷, 코위버 그리고 SKT가 지분을 투자한 ID Quantique-Korea 등이 국내 유선 QKD 상용화를 이끌고 있음
- SK텔레콤이 500억원을 투자하면서 2011년 국내 최초로 양자기술연구소 '퀀텀테크랩'을 설립함. 2016년 양자기술연구소는 세종시와 SKT 대전사옥 사이 유선 구간에 세계 최초로 QKD를 상용 LTE망에 적용함. 2019년부터 LTE·5G 백본망을 양자암호로 보호하기 시작했으며, 서울 성수 교환국사와 대전 교환국사 사이, 221km 구간에 QKD를 적용함. 2019년 11월 미국 괌·사이판 이동통신사 IT&E의 상용 LTE망에 QKD를 적용함.
- KT는 2017년 양자기술을 처음 연구를 시작하여, 국내 독자기술로 1년 만에 프로토타입을 완성하고, 국내 중소기업에 기술을 이전하여 상용 장비 제작. 2018년 1:N 구조를 적용한 다자간 QKD를 상용망 실증에 성공함. 2020년 상용 5G 네트워크에 양자암호통신 기술을 적용하고 2021년 고속 양자암호통신 기술개발에 성공함. 2022년 국내 최장거리(1KM) 무선 양자암호통신에도 성공함.
- 정부 차원에서 유선 QKD 장비를 국내 공공기관에 도입하기 위한 적합성 검증 정책이 2023년에 시행될 계획임

- 2023년 이후 국가 공공기관을 중심으로 유선 QKD망이 구성될 것으로 예상되며 이후 민간 망으로 점차 확대될 것으로 전망

o 2020년부터 양자암호통신 시범 인프라가 구축되어 유선 QKD 시스템의 보안성을 시범 검증한 결과로 국가용 보안 요구사항이 개발되었음. 이어 2023년에 국가 공공기관에 유선 QKD 시스템을 도입하기 위한 인증 제도가 시행될 예정임
- 2020년 SKT는 의료계 5G 양자암호 통신망을 구축함. 연세대학교 의료원 세브란스병원-강남세브란스병원-용인세브란스 병원 네트워크를 QKD로 연결하고, 특화 솔루션을 개발함.
- 특히, 2020년부터 광주시, 대전시 등 5개 기관 6개 구간, 연세의료원 등 6개 기관 11개 구간 등 총 17개의 공공·의료·산업분야에 양자암호통신 시범 인프라를 구축·운영하며 응용서비스를 발굴 적용함
- KT는 강원도청, 전남도청 등 5개 구간과 성모병원, 현대중공업 등 8개 구간, 그리고 공공·민간분야에 양자암호통신 시범인프라를 구축하고 운영중이며, 비화통신, 의료 정보보호, 자율주행차, 액화수소드론 등 다양한 응용서비스들을 적용함.
- QKD 시스템의 보안성을 시험하기 위한 보안 요구사항이 개발이 세계 최초로 이루어져 TTA 표준 제정됨(TTAK.KO-12.0356)

o 2021년 3월, 국가보안기술연구소와 표준과학연구원은 공동연구 결과 세계 최초로 도청이 불가능한 양자 직접통신을 실망 20km에서 구현 성공함
- QKD의 보안성을 검증하기 위한 상세 조건에 대한 개발 연구가 관련 산·학·연 협력 아래 이루어져 양자 키 분배 보안 요구사항이 세계 최초로 TTA 표준 제정됨(TTAK.KO-12.0356)
- 국정원은 2022년 ETRI, 국보연, TTA, NIA와 공공분야 양자암호(QKD 포함) 도입을 위한 보안적합성 검증기준을 세계 최초로 마련함

o 양자난수발생기(QRNG, Quantum Random Number Generator)는 양자 역학의 비결정론적 현상을 이용하여 완전 난수를 생성할 수 있는 기술임. 양자 정보 분야에서 QKD에 이어 국내 기업인 SK텔레콤과 EYL이 양자난수발생기(QRNG)의 상용화에 성공함. 양자난수발생기는 QKD에 비해 해외 선진기술과의 격차가 크지 않음
- SK텔레콤은 2015년 MWC 2015에서 5G 양자 암호화 시스템을 시연하고 양자난수발생기 칩을 개발하고 있다고 밝힌 이후 2017년 양자난수생성 칩 시제품 개발에 성공함.

- '19년 SKT는 5G 가입자 인증 서버에 QRNG를 적용함. 이를 통해 고객이 망에 접속해 인증받는 과정에서 개인정보보안을 한층 높였고, '20년에는 삼성과 협력하여 양자난수생성 칩을 적용하여 양자보안 기능을 제공한 "갤럭시 A퀀텀"을 출시함.
- '22년 6월, SK텔레콤은 비트리, KCS, 옥타코 등 암호 분야 기업들과 함께 QRNG로 보안을 강화한 제품을 개발해, 국방·공공 사업은 물론 글로벌 시장에 도전 비전 발표. '22년 6월에는 FIDO(Fast IDentity Online) 2차 인증 카드키에도 QRNG 칩셋을 적용함.
- EYL은 방사성 동위원소가 자연 붕괴되는 과정에서 발생하는 알파입자를 측정하는 방식으로 '16년 초소형 양자난수발생기(Micro Quantum Random Number Generator)를 칩으로 개발함.
- '21년 5월에는 QRNG와 암호기능을 원칩 형태로 집적한 고성능 암호칩 자체 개발에 성공함.
- '22년 양자난수를 USB, PCI, 서버에 적합한 기기로 제공하는 제품군, QRNG 기술과 암호기술을 SoC로 구현한 제품군, 양자난수를 활용한 독립형 암호화 장치를 시장에 출시하였음

o ETRI는 국내 최초 무선 QKD 시연 및 유무선 QKD 요소기술을 개발함
- 국내 최초 자체부품을 활용하여 275m 실환경에서 무선 QKD 시험 성공. 세계 최초 편광 부호화 집적화(편광빔 분리기, 반파장판, 빔분리기) 칩 기술 개발하여 새로운 무선 QKD 해킹 가능성 및 해결방법 제시
- '05년 25km 유선 QKD 시스템 시연 후, 유선 QKD 시스템 요소기술(GHz급 광원 및 검출소자 기반 초소형 유선 QKD칩/모듈)을 개발(KIST 공동)하고 있으며, 양자중계기 핵심요소기술인 양자얽힘 광원 및 단광자 광원 개발에 착수하였음('20년 이후 ~, POSTECH, KAIST, KIST 공동)

o KIST는 유선 QKD 네트워크 시스템 기술을 중심으로 프로토콜 및 핵심 부품 기술 확보
- '22년 장거리 QKD 프로토콜로 '18년에 영국 도시바 그룹에서 제안한 TF(Twin Field) QKD 연구에서, 세계 최초로 Star type 네트워크(2xN) 아키텍처를 제안하고 실험적으로 검증
- '19년 CMOS 이미지 센서 암전류를 이용한 난수발생기를 개발하고 '22년에 ㈜SDT에 기술이전하여 본격적인 상용화를 위한 제품 개발에 착수
- '22년 LiNbO3 박막 기반 QKD 양자광학계 칩 개발

o 국내 QKD 시험망 구축('20년~)

- QKD를 공공·민간 분야 26개 기관(대전상수도본부, 강원도청, ADT캡스, 현대중공업, 순천향대학교병원 등)에 시범 구축하여 실제망 운용 레퍼런스 확보
- 시범운용을 통해 공공기관에 QKD 운용 계획 수립: 행안부(국가융합망 SKB, '2022년~), 국방부(m-BCN KT, '23년~)

< 국내 기술 현황 >

구분	주요 내용
KT (우리넷, 코위버)	• Two-way 방식의 QKD 장비 개발(2018) - 국내 QKD 산업 생태계 확장 - 중소기업인 우리넷, 코위버에 QKD 기술이전 • 2021년 12월, 20kbps 고속 장비 개발 성공(2021) • 무선 QKD 시험 성공(2022년 5월) (2022) - 국내 최장 무선 양자통신 거리 달성(1km)
SKT (IDQ-Korea)	• 국내최초 양자기술연구소 설립(2011) • 단일광자검출, 간섭계 및 후처리 기술 확보(2013) • QKD 국가 시험망 구축(2016) • 세종시 상용 LTE망에 QKD 적용(2017) • SKT가 글로벌 양자암호통신 기업인 스위스의 IDQ사를 인수(2018) • EU 산하 프로젝트에서 양자암호 시험망 구축(2019) • 5G/LTE 백본망에 QKD적용 및 5G 가입자 인증서버에 QRNG적용 (2020) • 양자난수생성칩 출시및 삼성 갤럭시 A 퀀텀 스마트폰 출시(2020) • 상업용 QKD 장비 출시(Clavis300, 2020) • QRNG 탑재 갤럭시 퀀텀 2 출시 (2021)
ETRI	• 세계 최초 편광부호화 집적화칩 기술 개발(2017) • 국내 최초 무선 QKD 시험 성공 (약 300m)(2018) - 국내 기술로 무선 QKD의 가능성 증명 • 양자통신용 광원, 소형 마이크로 옵틱스 기반 편광복호화 모듈, 실리콘 단일 광자검출기 모듈 개발
KIST	• Two-way 방식의 QKD 시스템 (2013) 및 일대다 QKD 개발(2017) • TF-QKD 시험 성공(2022) • CMOS 이미지 센서 암전류를 이용한 난수발생기 개발(2019) • LiNbO3 박막 기반 QKD 양자광학계 칩 개발(2019)

[양자 컴퓨팅]

o 출연연 및 주요 대학을 중심으로 초전도, 이온트랩, 반도체 양자점, 고체결함, 광학 기반 양자컴퓨터 연구개발 진행 중

- KRISS와 성균관대에서 초전도 트랜스몬 5큐빗에 대한 동작 제어 및 싱글-샷 측정 수행
- 서울대에서 GaAs 4큐빗 소자의 단일 큐빗 동작 제어 및 싱글-샷 측정 수행 및 실리콘 5큐빗 소자 제작
- 서울대, 이화여대, 포항공대에서 이온트랩 양자컴퓨팅 하드웨어를 구축하고, 이온포획 및 단일 큐빗 제어 성공
- ETRI에서 실리콘 포노틱스 집적회로를 이용한 광자 기반 4큐빗 생성 및 CNOT 게이트 조작에 대한 특성 평가 수행

o 양자 알고리즘 및 양자정보이론에서 세계적 수준에 근접한 연구 수행중

- 출연연(ETRI, KIST 등) 및 주요 대학(서울대, 고려대, 연세대, KAIST, 성균관대 등)을 중심으로 양자 알고리즘 및 양자정보이론 분야에서 세계적인 수준에 근접한 연구를 활발하게 진행중
- ETRI는 최근 선형잡음문제를 해결할 수 있는 양자 알고리즘을 개발하여 양자내성암호 공략 가능성을 제시하였음. 이외에도 양자컴퓨팅 성능 평가 기술을 개발
- 서울대는 기계학습을 통한 새로운 양자 알고리즘 개발 및 고신뢰도 양자 하드웨어 최적화 연구 진행('19년~)

o 다양한 물리 시스템 기반의 양자 시뮬레이터 연구개발

- 출연연(KRISS, KIST 등) 및 주요 대학(서울대, KAIST, 성균관대 등)을 중심으로 중성원자 시스템, 광학계, 초전도 시스템을 기반으로 하는 양자 시뮬레이터 개발 연구 진행 중
- KAIST에서 20 큐비트급 리드버그 원자 기반 양자 시뮬레이터를 개발하여 NP-완전문제(최대독립집합 문제) 실험
- KIST는 계산화학 및 머신러닝 적용을 위한 광자 기반 양자 시뮬레이터 원천기술 개발 진행중('19년~, NRF 지원)
- KRISS는 대규모 양자소재 시뮬레이션을 위한 중성원자 기반 양자 시뮬레이터 원천기술 개발 진행중('19년~, NRF 지원)

o 한국형 양자컴퓨터 개발을 위한 투자 확대
- 상용화 수준의 양자컴퓨터 개발에 필요한 양자 프로세서, 알고리즘, 오류보정, 응용 SW등 4대 핵심 요소기술에 집중 투자 시작
- 50-큐비트급 한국형 양자컴퓨터를 조기 구축하여 단계적으로 고도화 추진 (KRISS, 성균관대, UNIST, KISTI)
  * 1단계('21~'24) : 50큐빗 양자 프로세서 확보
  * 2단계('25~'30) : NISQ 양자컴퓨터 확보
  * 3단계('31~'35) : 오류정정 범용 양자컴퓨터 확보

o 국내 양자 컴퓨팅 연구개발 지원을 위한 '양자정보연구지원센터' 설립
- 국내 양자 컴퓨팅 연구개발을 지원하기 위해 2020년 8월 성균관대학교 자연과학 캠퍼스에 '양자정보연구지원센터(https://qcenter.kr)' 설립
- 국내 양자 정보분야 신진연구인력 양성 및 저변확대를 위한 인력양성 사업 (박사후 연구원 지원, 양자정보과학 계절학교, 고등학생 및 일반인 대상 교육, 양자정보경진대회, 각종 교류 행사 및 세미나 개최 등) 진행
- 초전도 소자 일괄공정 서비스 제공 및 다양한 양자 소자 제작을 위한 단위 공정 서비스 제공을 목적으로 한 시스템 구축 중
- 국외 양자컴퓨터 클라우드 서비스(IBM, IONQ, D-Wave) 활용 및 국내 연구자 네트워킹 지원

< 국내 기술 현황 >

구분	주요 내용
KRISS	• 초전도체 기반 범용 양자컴퓨터(≥5 큐비트) 시스템 실증 • 다체 양자문제를 위한 초저온 단일원자 큐비트 양자 시뮬레이터 • 광자 기반 양자 컴퓨팅(7큐비트) 및 양자 네트워킹(6광자) • 다이아몬드 색중심 소자
KIST	• 2큐비트 고체결함(다이아몬드 NV센터) 상온 동작 이동형 양자컴퓨터 시스템 개발(2021년) • 6큐비트 고체결함(다이아몬드 NV센터) 큐비트 생성 및 전자-핵스핀 큐비트 iSWAP 게이트 구현(2021년) • 고효율 광 포집을 위한 다이아몬드 나노 구조물 연구(2020년) • 2큐 쿼츠 광자 양자시뮬레이터 기반 VQE 구현(2022년)
ETRI	• 실리콘 포토닉스 집적회로를 이용한 광학 기반 4 큐빗 생성 및 게이트 제어 • 양자 알고리즘, 컴퓨팅 이론, 시스템 소프트웨어, Full-Stack 양자컴퓨터 구현 기술 연구개발

구분	주요 내용
서울대	• 반도체 양자점 큐빗 개발(GaAs 4 큐빗, Si 1 큐빗) • 이온트랩 양자컴퓨팅 연구
성균관대	• 양자정보지원연구센터를 통한 국내 양자컴퓨팅 연구개발 지원 • 초전도 양자칩 연구개발
KAIST	• 100 큐빗급 리드버그 양자 시뮬레이터 개발 • 국내 최초 양자컴퓨팅 SW 관련 스타트업(큐노바) 설립
삼성전자	• 미국 벤처회사에 투자 시작('19년~) • 삼성종합기술원내에서 IBM과 협력연구 수행중
현대차	• IonQ와 협력을 통해 전기차 배터리 및 자율주행 자동차 기술에 양자컴퓨팅을 접목하는 연구 수행중

[양자 센싱]

o 양자센싱 기술은 여러 물리적 플랫폼에 걸쳐 기초연구부터 상용화까지 다양한 수준으로 출연연구소 및 대학을 중심으로 연구되고 있음

- 양자센싱 기술의 특성상 측정대상인 물리량이나 응용분야가 플랫폼 별로 상이하여 대부분 독립적인 연구가 수행됨
- 플랫폼은 고체 점결함*, 원자, 초전도 소자, 광자 플랫폼 등이며, 핵심기술 사이의 차이점은 크지만, 저잡음 레이저와 같은 광학 장비가 비교적 보편적으로 사용되어 관련 기반기술을 보유하고 있는 연구자들의 비중이 높음

  * 고체 점결함: 대표적으로 다이아몬드 내부의 질소-빈자리(NV) 불순물
- 원자 기반의 양자센싱 연구는 주로 국방 활용을 목적으로 함. ADD, 부산대, KRISS, 나노종합기술원 등이 원자기반 양자관성센서, 원자기반 자기장 센서, 칩스케일 원자시계 등에 대한 연구를 수행함
- 최근의 양자센서 개발사업을 통해 KRISS는 원자시계와 광간섭계를 이용하는 양자 중력계, 자기장(70 pT)-온도(25 μK) 동시 정밀측정 고체점결함(NV) 다이아몬드 양자센서, 나노역학계 기반 온칩 마이크로파 빗(comb) 발생 소자, 고농도 NV 스핀 기반의 실시간 전류 이미징 기술을 개발함
- 고려대는 고체점결함 양자자기장 이미징으로서 100nm 수준의 공간 해상도로 2차원 소자의 전류 이미지를 얻는 단일 NV 스핀 주사 탐침형 기술을 구현
- KIST는 III-V 반도체(ex. InGaAs) 기반의 양자점 광원을 제작하여 2개의 광원으로부터 동일 광자의 생성이 가능함을 보고하였음. 또한 단파 적외선(SWIR) 이미징용 센서인 1차원 PbS 포토다이오드 어레이를 개발함

- KAIST는 초소형 마이크로 공진기를 이용하여 온칩 형태의 마이크로파 생성 기술을 개발하였고, 5×10^{-13} 수준의 주파수 안정도를 보고함. 단일 모드를 갖는 압축 광자의 안정적인 생성 및 검출을 위한 기초연구가 진행됨
- ETRI와 부산대 등은 저주파 통신용 원자 기반 센서 개발 연구를 수행 중이며 약 140fT 수준의 감도를 보고함
- KRISS와 부산대는 6G 전자파 측정 표준을 위한 리드버그 원자 기반 고주파 전기장 측정 연구를, 충북대학교는 동일 플랫폼으로 생체 전기활동 모니터링을 위한 저주파 전기장 센싱 연구를 수행함

o 기술 성숙도가 높은 원자 및 초전도 소자 기반 양자센서 관련 기술의 경우 국내 산업계가 참여함
- KRISS의 초전도양자간섭소자(SQUID) 기반 생체자기측정 기술은 AMCG사에 이전되어 심자도시스템으로 개발, 식약처 품목허가 취득
- KRISS의 이터븀 원자광시계는 세계 협정시에 참여하는 다섯번째 나라로서 국제적인 시간·주파수 측정표준 유지에 기여함

< 국내 기술 현황 >

구분	주요 내용
KRISS	• 다이아몬드 양자 센서 자기장 및 온도 동시측정 • 원자 기반의 중력계 및 칩스케일 소형 원자시계 개발 연구 • 초전도 나노역학계, 스핀 앙상블 기반의 광-마이크로파 변환 기술 • 고체 점결함(NV) 기반 광시야 자기장 이미징 기술 • 초전도 양자간섭소자 기반 생체자기측정기술(뇌자도, 심자도) 상용화
부산대	• ADD와 공동으로 원자 기반의 양자관성센서 기술 개발 • 원자 기반 고주파 전기장 측정 표준 기술 개발(KRISS 공동) • 원자 기반 자기장 통신용 비차폐 RF 자기장센서 연구
고려대	• 고체 점결함(NV) 기반 단일스핀 주사탐침형 이미징 및 광시야 자기장 이미징 기술
ETRI	• 원자 기반 자기장 통신용 RF 자기장 센서 개발
KIST	• III-V 양자점 양자광원 및 SWIR 1차원 이미징 센서 개발 • 단일 전하 계측용 HEMT 개발 연구
서울대	• 고체 점결함(NV) 기반 고속 온도 센싱 연구
KAIST	• 압축 광원 기반의 양자 이미징 연구 • 온칩 초안정 마이크로파 생성 기술 개발
한양대	• 나노포토닉스 기반의 플라즈모닉 양자 센싱 기술 이론 연구
ADD	• 원자 증기 기반의 NMR 관성 센서 개발 • 얽힘 및 압축 광자 검출 이론 연구

[양자 네트워크]

o 양자 네트워크 기술은 양자컴퓨터, 양자 센서, 양자 암호시스템 등의 양자 디바이스를 양자 상태로 정보를 전달·교환하는 기술로 국내에서는 구현을 위한 기초 이론 및 실험 연구를 학교와 연구소 중심으로 진행

- Postech과 KIAS 공동연구로 양자전송 및 얽힘 치환 최적화 이론 및 구현 실험('21년)
- KIAS와 표준연 공동연구로 다자간 양자전송 및 양자 네트워크 방법론 개발('20년)
- KIST는 경희대와 공동연구로 다자간 양자 네트워크 실험연구 수행('20년)
- KIAS와 서울대 공동연구로 양자중계기 프로토콜 개발('19년)

o '22년, 양자 인터넷 관련 연구개발 과제 기획 및 '양자중계기 등 핵심 기술 개발사업' 추진(IITP)

- 양자인터넷을 위한 유/무선 양자 중계기 개발 과제('22~'26)
- 양자인터넷 구현 핵심기술인 양자 메모리 개발 과제('22~'26)
- 양자 기술 로드맵에 양자인터넷을 명시하고 R&D 지원체계 마련('22년, IITP)
- 양자 통신 로드맵에 양자네트워크를 명시하고 추진 방안 마련중('22년, 국가과학기술 자문회의 양자 특위)

< 국내 기술 현황 >

구분	주요 내용
KT	• 양자인터넷을 위한 유선·무선 양자중계기 개발 과제('22~'26, IITP) 참여 무선 양자채널 기술 개발('22년, 1km 검증)
SKT	• 양자인터넷을 위한 유선·무선 양자중계기 개발 과제('22~'26, IITP) 참여 양자 센싱 기술 개발
ETRI	• 양자인터넷을 위한 유선·무선 양자중계기 개발 과제('22~'26, IITP) 주관 양자인터넷 구현의 핵심 기술인 양자 메모리 개발 과제('22~'26, IITP) 주관
표준연, KIST, KIAS, POSTECH, 경희대, 서울대	• 양자 네트워크 구현을 위한 기초 이론 및 실험 연구

2.2.2. 국외 기술개발 현황 및 전망

[양자 암호통신]

o 해외 글로벌 기업들이 적극적 QKD 기술 연구 프로그램을 진행해오고 있음
- 스위스 ID Quantique를 시작으로 MagiQ Technologies, Inc.(미국), QNu Labs(인도), QuintessenceLabs(호주), QRate(러시아), SeQureNet(프랑스) 등이 상업적 QKD를 시장에 선보였으며, 도시바(유럽), HP, IBM, 미쯔비시, NEC, 일본전신전화(NTT) 기업 등이 있음
- BB84 프로토콜이 기본이었던 QKD 시장에 최근 COW(Coherent one-way) 프로토콜이 적용되기 시작함(ID Quantique, Clavis XG QKD system)
- QKD 프로토콜이 시스템화 되면서 나타나는 부채널 공격의 취약점을 해결하기 위한 MDI-QKD 프로토콜과 TF-QKD 등이 미래 QKD 프로토콜로 연구되고 있음
- 스위스 제네바에서 2001년 창립한 ID Quantique사를 필두로 호주의 QuintessenceLabs, 도시바 유럽 등 이미 QKD 기술은 상업화에 성공함
- 양자암호통신에 대한 중국의 국가적 투자는 양자기술 관련 특허가 3000건을 넘어서는 등 객관적 지표에서 미국의 2배 이상을 기록하며 중국이 2010년 중반 이후 양자통신의 선두주자로 발돋움함
- 2016년, 중국의 양자통신 전용 위성인 무쯔(Micius)를 시작으로 위성을 이용한 양자위성통신 시대가 개막됨
- 중국은 2021년 1월 통합 양자통신망 구축을 발표. 지상 700개 이상의 광섬유와 2개의 지상-위성 링크를 결합한 양자통신 네트워크 구축(총 4,600km에 걸쳐 양자키분배 성공함)
- 양자통신 기술 및 양자통신 전용 위성 수의 증가로 세계적인 네트워크가 형성되면 전 세계를 연결하는 양자 인터넷이 구현될 전망

o 2019년 9월, 유럽 국가에서는 산학연 총 38개 기관이 참여하여 다양한 모델의 QKD 장비를 연결하는 OPENQKD PROJECT를 시작함
- 프로젝트 목적은 이종 QKD 장비를 연결하여 네트워크를 구성하고 안전한 통신을 구현함으로 그 효용성을 검증 및 증명하고 최종적으로는 유럽 대륙에 QKD 네트워크를 구성하는 것임

o QKD의 보안성을 검증하기 위한 보안 요구사항 표준이 JTC1에서 진행되고 있으며 현재 막바지 단계인 DIS(draft international standard)에 이르렀음

o 난수성은 보안을 위한 핵심적인 요소로, 양자난수발생기는 실난수를 제공하는 물리적 기술로 난수발생기 시장의 혁신으로 받아들여져 해외에서는 일찍이 그 시장성을 내다보고 산업계의 연구가 활발히 이루어짐

- '16년도부터 IDQ에서 상용 QRNG를 출시하였으며, '22년 현재 네 종류의 HW가 공개되었으며, QRNG 칩을 포함하여 PCIe 슬롯과 USB 인터페이스를 지원하는 HW, 독립 장비 형태의 HW가 있음
- 최근 Quantum emotion사에서 세계 최초 회로 크기의 QRNG인 QNG2를 출시함. 실제 크기는 20X20 microns 이하로 1Gbps의 속도로 동작함
- 향후 저비용, 소형화, 고속 동작을 목표로 QRNG가 개발될 것으로 예상됨

o QKD 시스템 소형화 연구개발 현황

- QKD 시스템의 소형화를 위한 칩 기반 QKD 시스템 연구가 필요하고, 광 집적소자는 Si, SiO_2, InP, GaAs 등을 많이 사용하며, 광 변조기와 같은 능동 소자 구현도 가능함
- 캐나다 토론토 대학(Lo 연구팀)은 편광 인코딩 양자키분배를 위한 실리콘 칩 기반 송신부 개발하고, 구현된 칩은 표준 공정으로 제작되었으며 1.3mm x 3mm 영역에서 펄스 발생기, 강도 변조기, 가변 광 감쇠기 및 편광 변조기를 집적하였음
- 영국 브리스톨 대학(O'Brien 연구팀)은 InP 기반 양자키분배 송신기와 SiO_xN_y 기반 수신기를 공정하여 고속 양자키분배 수행. BB84를 포함한 coherent one way, differential phase shift 프로토콜의 양자키분배가 가능한 형태의 송수신부 칩 제안
- 미국 MIT 대학(Dirk Englund 연구팀)은 실리콘 기반 고속 편광 제어를 통해 양자키분배를 실제 환경에서 구동. 도심 43km 거리에서 157kbps의 비밀키 생성 속도 시연

< 국외 기술 현황 >

구분	주요 내용
미국, MagiQ	• 2003년에 상업용 QKD 제품(Navajo) 출시. 이어서 QPN 5505, QPN 7505, QPN 8505를 연이어 출시함 - 현재 상용 고객 및 정부 고객을 대상으로 시험과 측정, 광학 센싱, 통신시장에서 솔루션을 제공하고 있음
중국, Pan jianwei team	• 세계 최초 양자통신 전용 위성 발사 성공 - 2016년 8월 무쯔(Micius)호 - 양자위성을 이용한 양자 네트워크 구성 - 2017년 6월 위성과 지상 간 양자얽힘상태 공유 시험 성공 • 양자 네트워크를 구성하여 총 4,600km의 거리에 걸쳐 양자키분배 성공

구분	주요 내용
유럽, Toshiba EU	• 광 전송 거리 240km의 BB84 기반 QKD 개발 • 높은 키 전송률의 QKD 개발 - 2008년 1Mbps(20km) - 2012년 1Mbps(50km) - 2020년 13.7 Mbps(10km)
스위스, IDQ	• 2001년 스위스 제네바에서 설립하여 QKD 장비를 비롯하여 양자난수발생기, 양자 센싱을 개발하는 기업 - 2004년 QKD 상용 제품 출시 - 2007년에 스위스 제네바 지역 투표에 해당 사의 양자암호 기술을 이용 - 2014년, Quantum-Safe Working Group을 설립하여 정부와 기업에 네트워크에서 양자암호로 데이터를 보호하는 방법을 이해하도록 함

[양자 컴퓨팅]

o 거대 IT 기업과 양자컴퓨팅 전문 스타트업을 중심으로 치열한 범용 양자컴퓨터 연구개발 경쟁

- 거대 IT 기업(IBM, Google, Intel, 알리바바 등)들과 양자컴퓨팅 전문 스타트업(Rigetti, IonQ, Xanadu, PsiQuantum, ORCA, D-Wave 등)을 중심으로 NISQ 수준의 양자컴퓨터 구현 및 규모 확장을 위한 연구를 활발히 진행하고 있고, 궁극적으로는 오류정정이 적용된 대규모 내결함성 양자컴퓨터 구현을 목표로 연구개발 중
- 몇몇 기업을 중심으로 사용자 클라우드 서비스를 제공하고, 다른 기술 분야와의 협업을 통해 실생활 문제 해결에 양자 컴퓨팅을 활용하기 위한 시도를 진행 중
- 각국의 정부 연구소 및 선도 대학들을 중심으로 양자 컴퓨팅 이론 및 알고리즘 연구개발도 활발하게 진행됨

o 양자컴퓨터의 효용성 입증을 위한 '양자 우위(Quantum Supremacy)' 시연 경쟁

- '양자우위'란 양자컴퓨터의 계산능력이 월등히 뛰어나 어떠한 고전 컴퓨터로도 동등한 수준의 계산을 수행할 수 없는 경우를 말함
- Google은 지난 '19년 자사의 초전도 53큐빗 양자컴퓨터 프로세서(시카모어)를 사용하여 무작위 양자회로 샘플링 문제를 해결했다고 발표하였음
- Google은 양자컴퓨터로 해당 문제를 풀어내는데 200초의 시간이 소요되지만 현존 세계 최고 슈퍼컴퓨터(서밋)를 이용하면 10,000년이 소요될 것으로 추정

- 중국과학기술대학은 광자 76큐빗 양자컴퓨터를 이용하여 보존 샘플링 문제를 해결하였음
- 슈퍼컴퓨터로 해당문제를 풀 경우 25억년의 시간이 소요될 것으로 예상되지만, 중국과학기술대학 연구팀은 자체 개발한 광자 기반 양자컴퓨터를 이용해 불과 200초에 해결하였음(10^{23}배 우위)
- 이외에도 초전도 66큐빗 양자컴퓨터(조충지 2.1)를 이용해서 무작위 양자회로 샘플링 문제를 풀었음을 발표하였음(1,000배 우위)
- 캐나다의 포토닉스 기반 양자컴퓨터 개발 스타트업인 Xanadu에서 자사의 프로그래밍 가능한 클라우드 양자컴퓨터(Borealis)에서 보존 샘플링 문제를 불과 36 마이크로초에 해결하였음(슈퍼컴퓨터로 9,000년 소요 예상)

o 대규모 실생활 난제 해결에 요구되는 결함허용(오류내성) 양자컴퓨터 기술 확보를 위한 치열한 경쟁
- 양자물리 시스템이 갖는 근본적인 오류로 인해 실생활 문제 해결에 필요한 대규모 시스템 개발을 위해서는 양자물리 시스템의 고유특성에 기반해 개발된 양자오류정정 기술의 적용이 필요함
- 하지만, 양자오류정정 기술이 효과를 발휘하기 위한 특이 임계점이 존재하는데, 이를 만족시킬 수 있는 하드웨어 개발 연구와 임계값을 낮추기 위한 이론 및 소프트웨어 연구가 광범위하게 진행되어 왔음
- Google에서 중요한 실험 결과를 '21년과 '22년에 잇따라 발표하였는데, '21년에는 자사의 초전도 큐빗 프로세서(시카모어)를 활용하여, 반복 부호 기반의 실험 결과를 발표하였는데, 논리 큐빗의 블록 크기가 증가함에 따라 논리적 오류율이 감소함을 보임
- '22년에는 상기 프로세서의 규모를 확장하여 부호길이 3과 5의 surface code 양자오류정정 실험을 수행하고, 부호길이 확장에 따라 평균적인 논리적 오류율이 감소함을 보였음
- 이온트랩 기반 양자컴퓨터를 개발하고 있는 Honeywell 에서는 '21년 자사의 10-큐빗 양자 컴퓨터를 이용하여 [[7,1,3]] Steane code에 대해 실시간으로 양자오류정정 반복 실험 수행 결과를 발표하였음

o 미국/유럽을 중심으로 한 광범위한 양자 시뮬레이터 기술 개발
- 미국과 유럽이 양자시뮬레이터 연구를 주도하고 있으며, 원자 플랫폼의 양자다체문제 해결, 광자 플랫폼의 보존샘플링 기반 양자화학 에너지 레벨 문제 해결 등에 주력하고 있음

- 양자 어닐러 클라우드 플랫폼 Leap2 발표('20년, D-Wave)
- 알칼리 원자 양자 플랫폼을 이용한 하버드 모델 양자시뮬레이션('20년, Harvard, MPQ)
- 알칼리 토금속 원자를 이용한 양자자성 모델 양자시뮬레이션 ('20년, NIST)

< 국외 기술 현황 >

구분	주요 내용
미국, IBM	• 127 큐빗 수준의 초전도 양자컴퓨터 개발 • '23년 1000 큐빗 규모, '25년 4000 큐빗 규모 양자컴퓨팅 프로세서 개발 계획 발표 • 양자컴퓨팅 클라우드 서비스 제공, Qiskit을 비롯해 양자컴퓨터 상용화 • 양자컴퓨팅 핵심 이론 연구 수행
미국, Google	• 53 큐빗 초전도 양자칩 시카모어를 활용한 양자우월성 입증('19) • Surface code(d=3, 5) 기반 양자오류정정 입증('22) • Tensorflow Quantum 양자기계 학습툴과 qsim, cirq 등 양자컴퓨팅 연구개발 소프트웨어 발표 • '29년까지 100만 큐빗(1,000 논리 큐빗) 범용 양자컴퓨터 구축 계획 발표 • 상업용 양자컴퓨팅 SW 개발 스타트업 샌드박스(Sandbox AQ) 분사
미국, Rigetti	• 80 큐빗 수준 초전도 양자컴퓨터 개발(모듈식 양자칩) • '25년 1,000 큐빗, '27년 이후 4,000 큐빗 양자컴퓨팅 시스템 개발 계획 발표
중국, USTC	• 66 큐빗 초전도 양자컴퓨터(Zuchongzhi 2.1) 개발 • 60 초전도 큐빗 규모 양자 우월성 증명 실험 • 113 광자 보존 샘플링 적용한 양자 우월성 증명 실험
미국, IonQ	• 32 큐빗 규모 이온트랩 기반 양자컴퓨터(Forte) 개발 • MS, Google, Amazon을 통해 양자컴퓨팅 클라우드 서비스 제공 • '28년까지 양자이점 확인 로드맵 발표
미국, Quantinuum	• 12 큐빗 이온트랩 양자컴퓨터(H1-2) 개발(양자볼륨 4,096, 2-큐빗 게이트 신뢰도 99.81%)
미국, Intel	• QuTech(네덜란드)와 공동으로 초전도 및 반도체 양자점 큐빗 공동 연구(현재는 양자점 큐빗에 집중) • 자체 소프트웨어 개발 키트 (SDK) 개발 등 Full-Stack 양자컴퓨터 연구 • 양자 프로세서 제어를 위한 Cryo-CMOS 칩 발표('19, '20) • 양자컴퓨터용 미래 암호 기술 개발을 위한 '크립토 프론티어 연구센터 설립 발표
미국, Microsoft	• 양자컴퓨팅 알고리즘, 프로그래밍 환경(Q#, Liqui 등) 등 양자컴퓨팅 소프트웨어 연구 • 전세계 실험 연구팀과 활발한 협력 연구 수행

구분	주요 내용
미국, Amazon	• 양자컴퓨팅 서비스(Amazon Braket) 출시
캐나다, D-wave	• 양자 어닐링 방식 5000 큐빗급 양자컴퓨터 개발
네덜란드, QuTech	• Intel과 초전도 큐빗 및 반도체 양자점 큐빗 협력 연구 • 고체결함 양자컴퓨터 연구 개발, 7개 큐빗 얽힘 구현
캐나다, Xanadu	• 연속변수 기반 216 압축상태(squeezed-state) 큐빗으로 양자우월성 입증(Borelis)

[양자 센싱]

o 소형화와 집적화를 통해 실용성을 높이는 칩스케일 원자시계 및 원자기반 중력·가속도 센서 개발

- 2000년대 초반 미국 DARPA CSAC(Chip-Scale Atomic Clock) 프로그램을 통한 NIST 주도의 칩스케일 원자시계 개발의 결과로 MicroSemi, AOsense 등의 기업이 탄생함
- DARPA는 현재 QuASAR 프로그램을 통해 양자 표준한계에 근접하는 양자 센싱의 핵심기술 개발을 지원하고 있으며, 이 기술을 생체 이미징, 관성 항법 등에 응용하고자 함
- 프랑스 SYRTE는 감도 및 정확도가 고전중력계(FG5) 보다 뛰어난 양자 중력계를 구현하고 2018년 MuQuans사를 설립하여 이동형 중력계 판매 중
- 영국은 UK Quantum Technology Hub 중 Birmingham 대학 주축의 Sensors and Timing 디비전이 원자 기반의 자기장 및 중력계 기술개발을 지원하며, 2013년 Quantum Initiative 프로그램을 통해 개발된 원자 기반 중력계는 M-Squared 사에서 판매하고 있음

o 원자 증기셀을 이용하는 자기장 및 고주파 전기장 센서 응용기술 개발과 사업화 추진

- 2000대 중반 이후 NIST와 프린스턴대가 개발한 원자 증기 셀 기반의 소형 자기장 센서 기술이 상용화되면서 SQUID에 필적하는 감도의 원자자력계 센서를 판매하는 기업(QuSpin, Twinleaf, Fieldline)들이 만들어짐
- 원자 기반 고주파 전기장 센싱의 Rydberg Technology, 단파적외선(SWIR) 이미징 센서의 SEE Device, Infinity Electro-Optics, 광공진기 기반 가스 검출 기술의 Entanglement Technologies 등 기업들이 북미 지역에서 탄생

o 다이아몬드 색중심 기반 양자센서의 기초 및 응용연구와 이를 위한 다이아몬드 소재와 광·마이크로웨이브 제어시스템 사업화

- 하버드 대학을 중심으로 한 양자센싱 및 이미징 연구의 결과로 Lockheed Martin에서는 GPS jamming을 대비한 다이아몬드 지자장 센서를 개발하였고, ODMR technologies, Quantum Diamond Technologies, SBTech(캐나다) 등의 관련 기업이 등장했으며, ADAMAS, BIKANTA 등의 기업들이 나노 다이아몬드를 판매함
- 유럽은 EU Quantum Flagship 프로그램을 통해 유럽이 강점을 보이는 다이아몬드(NV) 센싱의 응용 연구(ASTERIQS)를 지원하고, 동시에 원자 기반 기술(iqClock, macQsimal)과 같이 상대적으로 뒤쳐진 분야를 육성함. Thales, Teledyne, Bosch 등의 유럽 대형 기업이 참여하여 상용화 수준의 솔루션을 개발하도록 유도함
- 영국 민간 기업인 Element Six와 Warwick 대학과의 공동연구를 통해 개발된 고순도 CVD 다이아몬드 기판 및 NV 다이아몬드가 전세계 양자기술용 다이아몬드 시장에서 독점적 위치를 갖고 있음
- 스위스의 Basel 대학과 ETH가 독립적으로 설립한 Qnami와 QZabre에서 세계 최초로 NV 단일스핀 기반 주사탐침 프로브 및 자기장 이미징 시스템을 개발하여 판매하고 있고, Zurich Instrument에서 양자 센싱 및 컴퓨팅의 핵심인 다채널 MW, AWG 등의 장치들을 판매함

< 국외 기술 현황 >

구분	주요 내용	활용 센서
미국, MicroSemi, AOsense, Quspin, Twinleaf, Fieldline, Rydberg Technologies	• MicroSemi, AOsense - 칩스케일 원자시계 • Quspin, Twinleaf, Fieldline - 소형 원자자력계 센서 • Rydberg Technologies – 고주차 전기장 측정 시스템	원자
미국, Quantum Diamond Technology, Lockheed Martin, Adamas, Bikanta	• Quantum Diamond Technology – 고속 바이오 마커 검출 기술 • Lockheed Martin – 자기장 항법 용 다이아몬드 자기장 센서 • Adamas, Bikanta – 형광나노다이아몬드	다이아몬드
미국, SEE Devices, Infinity E&O, Entanglement Technologies	• SEE Devices, Infinity E&O – SWIR 이미지 센서 • Entanglement Technologies – 양자 가스 검출기	광자, 이미징

구분	주요 내용	활용 센서
영국, Birmingham, M Squared	• Birmingham 대학 – 원자 기반 양자 센서 개발 • M Squared – 원자 기반 양자중력계	원자
영국, ElementSix	• ElementSix – 고순도다이아몬드 기판, NV 다이아몬드 센서	다이아몬드
스위스, Qnami, Qzabre, Zurich Instrument	• Qnami, Qzabre – 단일 NV 스핀 주사탐침 현미경 및 이미징 시스템 • Zurich Instrument – 다채널 MW source, AWG	다이아몬드
프랑스, MuQuants	• MuQuants – 원자기반 양자중력계	원자
독일, Qutools	• Qutools – 교육용 다이아몬드 양자 센서 시스템	다이아몬드

[양자 네트워크]

o 양자 네트워크 기술은 양자 컴퓨터, 양자 센서, 양자 암호시스템 등의 양자 디바이스를 양자 상태로 정보를 전달·교환하는 기술로 미국과 유럽에서는 국가단위의 차세대 기술 확보 대상으로 선정되어 시험망 구축에 착수하는 등 기술개발이 본격적으로 시작되고 있음

- 유럽의 EU 27개 모든 회원국이 참여하는 EuroQCI 프로그램이 Digital Europe 프로그램 재원을 통해 범유럽 유선·무선·위성 양자 인터넷 인프라 구축을 목표로 '21년부터 추진 중임
- 또한, 유럽 내 30여 산학연 생태계를 기반으로 Quantum Internet Alliance가 출범하여 양자 프로세서-양자 네트워크 인터페이스를 포함하는 양자 네트워크 기술 개발에 주력하고 있음
- 미국은 시카고 지역에 총 6개의 노드를 연결하는 120마일 거리의 Quantum Network 테스트베드를 구축하고 기술검증에 활용하고자 함('22년)
- 네덜란드 TU Delft 산하 QuTech은 암스테르담과 헤이그를 연결하는 양자 네트워크 테스트베드를 구축하고, 양자리피터 개발 및 양자인터넷 Protocol Stack을 제안하는 등 기술선점에 주력하고 있음('21년)
- 일본은 '19년 학계 위주의 Quantum Internet Task Force를 신설하고, '20년 양자 이노베이션 국가전략에서 양자센서/컴퓨터 기술개발을 위한 중장기 계획을 추진했으나, 최근 양자인터넷 조기 구현을 위한 표준화, 스타트업 육성, 응용분야 발굴 등으로 방향을 전환했음

o 양자 네트워크는 차세대 국가 사회경제 플랫폼으로 예상되고 있어, 양자기술 선진국은 국가 정책 및 기술개발 방향성을 양자인터넷 구현에 맞추고 기술력 확보에 경주를 하고 있음

- 지금까지는 양자 메모리, 양자 리피터 등과 같은 요소기술 위주 연구개발에 주력해왔으나, 최근에는 양자네트워크 시험망 구축·운영을 통한 네트워킹 기술과 표준화, 그리고 시장확보를 위한 응용서비스 발굴에 주력하는 중임
- 최근, 기술패권 경쟁 트렌드를 감안하면 미국의 현재 인터넷 커버넌스를 양자 인터넷에서도 유지하기 위한 표준화 선점 및 구현 노력과 더불어 이에 대항하는 유럽/아시아의 대응이 치열히 전개될 것으로 전망됨.

< 국외 기술 현황 >

구분	주요 내용
스페인, ICFO (Institute of Photonic Sciences)	• 25 마이크로세컨드 간 저장 가능한 양자 메모리 구현 • 10m 간격의 두 양자 메모리 대상 얽힘 적용
중국, USTC (University of Science and Technology of China)	• 3.5m 간격의 두 양자 메모리 간 중간노드 기반 BSM 구현 성공하고, 양자 리피터 구현 연구개발 중
네덜란드, TU delft	• 세계 최초 양자 네트워크 시험망 구축 • 양자 인터넷 프로토콜 스택 제안 • 양자 네트워크 OS 개발 (QNodeOS)
미국, 아르곤연구소	• 아르곤연구소와 페르미연구소간 50km 거리의 양자 네트워크 시험망 구축 - 분산형 양자 컴퓨팅 환경 제공
미국, IETF/IRTF	• 양자인터넷 표준 개발을 위한 기본 문서 2건 작성 중 - Architecture principle 및 Use Cases
국제기구, ITU	• ITU-T FG QIT4N 설립('20년) 이후 양자 네트워크 표준화를 주요 후속 표준주제로 제언 - ITU-T SG13에서 TR.QEFN(Quantum Enabled Future Network) 표준화과제에서 양자 인터넷 개발 착수

2.3. IPR 현황 및 전망

o 특허분석 개요

- (기술의 내용) 양자정보통신 기술의 16개 표준화 항목(7개 중점 표준화 항목 포함*)의 키워드 고려하여 분석을 수행함.

  * 양자키분배(QKD) 시험 인증 표준, 양자키분배 네트워크 및 망관리 표준, 양자키분배 시스템 표준, 양자키분배 프로토콜 및 키관리 표준, 양자 컴퓨팅 용어 표준, 양자 네트워크 구조 표준, 양자 전송 기술 표준

- (분석 대상 및 범위) 분석 대상은, IP5(한국, 미국, 일본, EPO 및 중국)으로 한정하였고, 출원일자를 기준으로 하여 '02년 7월 1일 ~ '22년 7월 27일까지 등록 또는 공개된 특허로 한정하여 중점 표준화 항목별로 검색 및 추출된 총 3,525건[1]의 특허를 대상으로 분석함

  * 일반적으로, 특허는 특허출원 후 18개월이 경과된 때에 출원 관련 정보를 대중에게 공개하도록 하고 있으므로, 2020년 말부터 출원된 특허는 미공개 상태에 있을 것으로 추정됨

< 양자정보통신 분야 특허분석 범위 >

국가	검색DB	분석구간	검색범위	핵심키워드
한국(KR)	WIPS	2002.07.01.~ 2022.07.27.	특허 공개 및 등록 전체문서	Quantum authentication signature error correction communication cryptography secure security key encryption distribution trusted network "QoS" circuit qubit coherence compile neural rydberg annealing accelerometer gravity rotation gyroscope clock frequency
미국(US)				
일본(JP)				
유럽(EP)				
중국(CN)				

1) 우선권 주장 제도를 통해 하나의 발명을 여러 국가에 출원할 수 있고, 우선권 주장 제도로 묶인 특허 출원들(소위 패밀리 특허)은 하나의 특허 출원으로 보고 계산한 숫자임. 패밀리 특허를 이루는 개별 특허들의 합은 4,419건임.

국가	검색DB	분석구간	검색범위	핵심키워드
				entanglement imaging microscope spectrometer interferometer light

o 양자정보통신 분야 특허 다출원 5개국 연도별 특허출원 동향

< 주요국 특허 통계(2002~2022) >

(단위 : 건)

구분	한국(KR)	미국(US)	일본(JP)	유럽(EP)	중국(CN)	합계
2002	3	14	9	10	3	39
2003	2	20	14	9	8	53
2004	2	23	22	17	7	71
2005	4	20	21	9	6	60
2006	4	24	27	15	7	77
2007	0	14	27	5	2	48
2008	3	19	11	12	4	49
2009	7	19	20	11	14	71
2010	4	15	17	6	22	64
2011	4	21	8	10	26	69
2012	10	20	11	8	38	87
2013	8	28	15	11	72	134
2014	14	31	19	9	73	146
2015	25	44	24	25	104	222
2016	23	47	23	29	164	286
2017	31	39	16	26	307	419
2018	30	51	11	24	461	577
2019	43	69	4	34	534	684
2020	35	97	9	28	480	649
2021	19	50	1	9	389	468
2022	1	12	1	1	131	146
합계	272	677	310	308	2852	4419

- 양자정보통신 기술 분야에서 출원 활동은 2010년 중반대 이후부터 활발해졌고, 중국 중심으로 활발히 이뤄지는 것으로 파악됨. 특히, 미국, 일본, 유럽의 출원 활동을 비교하면, 미국을 중심으로 출원 활동이 활발하게 포착되었고, 일본,

유럽의 출원 활동은 비슷한 수준으로 파악됨. 한국은 다른 국가들 대비 출원 활동이 상대적으로 높지 않은 것으로 파악됨.

o 양자정보통신 기술 분야 구간별 주요 IPC* 특허출원 동향

< 구간별 주요 IPC 통계 >

(단위 : 건)

구분**	H04L-009/08	G06N-010/00	H04B-010/70	H04L-009/32	H04L-029/06	G06N-099/00
2012~2014년	45	8	40	2	3	8
2015~2017년	112	34	77	4	23	14
2018~2020년	133	109	52	21	3	3

* IPC(International Patent Classification, 국제특허분류): 섹션(Section), 클래스(Class), 서브클래스(Subclass), 메인그룹(Maingroup), 서브그룹(Subgroup)으로 이루어진 5단계의 계층 구조를 가짐

- H04L-009/08 기술 분류(키분배) 내에서, 2015년 이후 꾸준한 특허 출원 활동이 포착됨. 이외, 양자 컴퓨터 시스템 일반 분류(G06N-010/00)에서 2018년 이후 출원 활동이 급격히 증가된 것으로 파악됨.

< IPC 완전분류기호 >

- **H04L-009/08** : 키 분배(key distribution)
- **G06N-010/00** : 양자 컴퓨터, 즉 양자 기계 현상에 기초한 컴퓨터 시스템
- **H04L-009/00** : 비밀 또는 보안통신을 위한 배치
- **H04L-009/32** : 시스템 사용자의 신원(Identity)과 권한(authority)을 확인하는 수단을 가진 것
- **H04L-029/06** : 프로토콜에 의해 특징된, 배열, 장치, 회로 또는 시스템
- **G06N-099/00** : 특정 계산모델 방식의 컴퓨터 시스템에서, 이 서브클래스의 다른 그룹으로 분류되지 않는 주제사항

o 양자정보통신 분야 구간별 국내 주요 출원인 특허출원 동향

< 구간별 국내 주요 출원인 통계 >

2012~2014년			2015~2017년			2018~2020년		
출원인	건수	순위	출원인	건수	순위 변동	출원인	건수	순위 변동
ID QUANTIQUE	7	1	한국과학기술원	8	▲6	주식회사 케이티	18	NEW
SK TELECOM	5	2	ID QUANTIQUE	7	▽1	한국과학기술연구원	8	▲2
NEC	4	3	경희대학교 산학협력단	7	NEW	한국과학기술원	8	▽2
QUALCOMM	3	4	한국과학기술연구원	7	▲3	한국전자통신연구원	8	▲2

2012~2014년			2015~2017년			2018~2020년		
출원인	건수	순위	출원인	건수	순위 변동	출원인	건수	순위 변동
UNIVERSITE DE GENEVE	2	5	ALIBABA GROUP	5	▲4	주식회사 디지트로그	6	NEW
고려대 산학협력단	2	6	한국전자통신연구원	5	NEW	주식회사 이와이엘	6	NEW
한국과학기술연구원	2	7	HUAWEI	3	NEW	경희대 산학협력단	5	▽4
SAMSUNG	2	8	UNIVERSITY OF SEOUL INDUSTRY COOPERATION FOUNDATION	3	NEW	LG	2	NEW
ALIBABA GROUP	1	9	UNIVERSITE DE GENEVE	2	▽4	UNIVERSITY OF SEOUL INDUSTRY COOPERATION FOUNDATION	2	▽1
고려대 산학협력단	1	10	고려대 산학협력단	2	-	국민대 산학협력단	2	NEW

* 국내 주요 출원인 통계(2002~2022) 누적 수치는 요약보고서에서 확인 가능함

- 2012년 내지 2014년 시간 구간에서는, 외국 출원인(ID QUANTIQUE)을 중심으로, 국내 산학, 및 대기업(삼성전자)이 점유하고 있었으나, 이후 출원인 pool이 증가되었음. 국내 연구소(한국과학기술원, 한국과학기술연구원, 한국전자통신연구원) 및 산학협력단 중심의 출원 활동이 포착되고 있으며, 국내 기업은 국내 통신 사업을 주도하는 대기업(KT, SKT), 및 중소기업(이와이엘, 디지트로그 등)이 2018년 이후 출원 활동을 개시한 것으로 판단됨. 즉, 국내 기업이 2018년 이후 해당 기술에 대하여 관심을 갖기 시작한 것으로 판단됨.
- 한국의 주요 출원인은, 국내 연구소인 한국전자통신연구원, 한국 과학기술연구원, 한국과학기술원이 2018년 이전까지 활발히 출원하였던 것으로 포착됨. 한국 기술 시장에 관심있는 외국 출원인은 스위스 기업(ID QUANTIQUE), 중국 산학(칭다오 테크놀로지컬 대학)이 포착됨.
- 세부적인 출원을 살펴보면, “양자키 할당 우선 순위를 고려하는 양자 통신 시스템, 장치 및 방법(주식회사 케이티, 출원번호 10-2020-0007891)”, 및 “양자 키 분배 시스템 및 그 동작 방법(한국전자통신연구원, 출원번호 10-2021-0102626)”과 같이, 양자 키 분배 및 할당과 관련된 기술들이 주로 출원되고 있는 것으로 관찰됨.
- 2018년을 기점을 QKD와 QRNG를 중심으로 산업화가 진행되면서 기업들의 기술확보 경쟁이 특허 출원 통계에서 뚜렷이 나타남. 앞으로 국내 기업뿐만 아니라 외국계 기업들이 국내 특허 경쟁에 참여하여 특허 출원이 급격히 늘어날 수 있음.

o 양자정보통신 분야 구간별 국외 주요 출원인 특허출원 동향

< 구간별 국외 주요 출원인 통계 >

2012~2014년			2015~2017년			2018~2020년		
출원인	건수	순위	출원인	건수	순위 변동	출원인	건수	순위 변동
ANHUI ASKY QUANTUM TECHNOLOGY	18	1	ALIBABA GROUP	57	NEW	RUBAN QUANTUM TECHNOLOGY	156	NEW
KABUSHIKI KAISHA TOSHIBA	17	2	ZHEJIANG SHENZHOU LIANGZI NETWORK SCIENCE & TECHNOLOGY	44	NEW	QUANTUMCTEK	126	▲1
ZHEJIANG GONGSHANG UNIVERSITY	16	3	QUANTUMCTEK	42	▲1	CHINA ACADEMY OF ELECTRONICS AND INFORMATION TECHNOLOGY OF CETC	80	NEW
QUANTUMCTEK	11	4	ANHUI ASKY QUANTUM TECHNOLOGY	34	▽3	BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS	53	▲5
SK TELECOM	10	5	KABUSHIKI KAISHA TOSHIBA	33	▽3	NANJING RUFAN QUANTUM TECHNOLOGY	48	NEW
CHANGCHUN UNIVERSITY	9	6	ZHEJIANG QUANTUM TECHNOLOGIES	28	NEW	BEIJING ZHONGCHUANGWEI NANJING QUANTUM COMMUNICATION TECHNOLOGY	45	NEW
LOS ALAMOS NATIONAL SECURITY	9	7	ID QUANTIQUE	27	NEW	CENTRAL SOUTH UNIVERSITY	34	NEW
QUALCOMM	9	8	HUAWEI	26	NEW	CHENGDU UNIVERSITY OF INFORMATION TECHNOLOGY	34	NEW
NOKIA TECHNOLOGIES	8	9	BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS	19	NEW	INTEL	26	NEW
SHANGHAI LANGYAN OPTOELECTRONICS TECHNOLOGY	8	10	HENGTONG QASKY QUANTUM INFORMATION RESEARCH INSTITUTE	19	NEW	WELLS FARGO BANK	24	NEW

* 국외 주요 출원인 통계(2002~2022) 누적 수치는 요약보고서에서 확인 가능함

- 2015년 이후 2020년까지 신규 진입한 출원인이 1개 출원인(Wells fargo bank)을 제외한 모든 출원인이 중국 출원인으로 나타나, 본 기술 분야에 대하여 가장 많은 관심을 가진 국가는 중국인 것으로 판단됨. 특히 2018~2020년 구간에서는, 상위 10개 출원인 중 7개의 중국 출원인이 새롭게 진입하였음.
- 중국 국적의 출원인(QUANTUMCTEK(기업), RUBAN QUANTUM(기업), CETC(China Electronics Technology Group Corporation)(기업) 등)의 출원

활동이 활발하게 포착되었으며, 2018년부터 출원 건수가 급증한 것으로 분석됨. 중국 외 출원인으로는 일본 기업 출원인(NEC, TOSHIBA)이 포착됨.

- 세부적인 출원을 살펴보면, “Communication system and communication method based on quantum key card arrangement(RUBAN QUANTUM TECHNOLOGY Co.,Ltd, 출원번호 CN 2021-10868345)”, “Secret key refreshing system and method in quantum secret communication system(RUBAN QUANTUM TECHNOLOGY Co.,Ltd, 출원번호 CN 2020-11039050)와 같이, 양자 키와 관련된 기술이 관찰되어, 국내외 모두 양자 키 기술을 중심으로 출원이 수행되고 있는 것으로 파악됨.
- 중국의 양자기술에 대한 대대적인 투자가 특허 출원으로 나타남. 여기에 주요 선진국들이 경쟁에 뛰어들며 다국적 출원 경향성이 보임.
- 연구 단계에서 벗어나 산업화가 이루어지면서 산업계가 기술 확보를 위한 경쟁적 특허 출원이 확인됨. 이러한 경쟁은 세계적으로 양자기술에 대한 관심이 고조됨에 따라 더욱 심화될 것으로 예상됨.

2.4. 표준화 현황 및 전망

구분	상대표준수준(100%)				
	한국	미국	일본	중국	유럽
표준수준	90	80	90	90	100
※ 표준 수준은 "ICT 기술 및 표준 수준 조사" 설문조사에 의한 결과 값을 활용					

2.4.1. 국내 표준화 현황 및 전망

o 단체표준(TTA)

- TTA 광전송 프로젝트 그룹(PG201)
  - 광전송 기술에 대한 표준화를 진행하는 프로젝트 그룹으로, 전달망 구조 기술, 액세스망 기술, 광소자 및 광케이블 기술 같은 물리 인프라 기술과 관련된 표준 개발 중
  - 양자암호통신 네트워크 관련 ITU-T SG13, ETSI ISG QKD에서 개발된 국제표준의 영문 준용 표준과 KT 자체개발 양자암호 전달 네트워크 기능 구조 표준 등 총 15건의 표준이 개발 완료되었음
  - 양자암호통신 소프트웨어 정의 네트워킹 제어 관련 표준 등 3건의 표준을 현재 개발 중
- TTA 정보보호 기반 프로젝트 그룹(PG501)
  - 암호기술에 대한 표준화를 진행하는 프로젝트 그룹으로, 암호알고리즘/프로토콜, 양자정보통신의 암호키 관리, 암호 응용기술, PKI 시스템, OTP 기술, 인증/접근제어 및 권한 관리 기술 등의 표준 개발 중
  - 2018년 양자 키 분배 기술에 대해 일반적인 모델과 절차를 제시하고, 대표적인 양자키분배 프로토콜인 BB84 프로토콜에 대한 절차를 제시하는 2개의 표준이 완성되었음
    * 현재 개발중인 표준은 없으며, 추후 표준화가 필요한 프로토콜들이 많아지면 개발될 가능성이 있음
- TTA 사이버보안 프로젝트 그룹(PG503)
  - 사이버보안 기술 관련 표준화를 진행하는 프로젝트 그룹으로, 클라우드 컴퓨팅, 미래 인터넷, 스마트 모바일 네트워크 보안, 사이버보안 기술, 사이버 범죄 대응 기술(디지털 포렌식) 등의 표준 개발 중
  - 네트워크 보안을 위해 개발된 IPsec(IP 보안프로토콜) 장비에 양자키분배 장치에서 제공하는 양자 암호키를 적용하기 위한 표준 1건이 개발중
    * 추후 다양한 보안 네트워크 장비에 적용을 위한 표준들이 개발될 가능성이 있음

- TTA 응용보안/평가인증 프로젝트 그룹(PG504)
  - 금융보안, IoT, 클라우드 컴퓨팅, 스마트 그리드, 스마트 워크, 디지털 저작권 보호 기술 등 응용/융합 보안기술과 응용/융합 보안을 지원하는 구현/관리 지침, 정보보호관리체계(ISMS), 공통평가기준(CC), 암호모듈 검증(CMVP) 등 보안성 인증 및 평가기술에 대한 표준 개발 중
  - 양자 키 분배 시스템의 안전성을 보장하기 위한 요구사항 표준이 완성되어 있음
    * JTC1 SC27 WG3에서 개발중인 양자키분배 시스템 보안요구사항/시험요구사항 국제표준의 개발상황에 따라 추가적인 표준들이 개발될 가능성이 있음
  - 현재 표준화 과제로 스마트 그리드 보안 요구사항, 도로교통인프라 통합보안센터 보안 요구사항, 스마트시티 플랫폼 소프트웨어 보안 요구사항, 암호모듈 시험기술표준 사용지침 등이 진행 중임
  - 2023년도에 양자키분배 시험요구사항 표준의 과제 제안이 진행될 예정임

o 포럼표준

- 미래양자융합포럼
  - 양자 분야의 산·학·연 교류를 통해 양자 분야 생태계 활성화를 촉진하기 위한 포럼으로 TTA PG201(광전송 프로젝트 그룹)과의 협업을 통해 양자키 분배망 관련 표준들을 함께 개발하고 있음

< 국내 표준화 현황 >

표준화기구	표준(안)명	완료연도
TTA PG201	2019-1309, 양자 키 분배-REST 기반의 키 전달 응용 프로토콜과 데이터 형식	진행중 (2023)
	2022-0616, 양자 키 분배(QKD); 소프트웨어 정의 네트워킹을 위한 오케스트레이션 인터페이스	진행중 (2023)
	TTAE.IT-Y.3806, 양자키 분배망 – 서비스 품질 보장 요구사항	2022
	TTAE.IT-Y.3807, 양자키 분배망 – 서비스 품질 파라미터	2022
	2021-2357, 양자키 분배망 – 소프트웨어 정의 네트워킹 제어	2022
TTA PG201	TTAE.IT-Y.3801, 양자키 분배망 기능적 요구사항	2021

표준화기구	표준(안)명	완료연도
TTA PG201	TTAE.IT-Y.3802, 양자키 분배망 – 기능 구조	2021
	TTAE.IT-Y.3804, 양자키 분배망 – 제어 및 관리	2021
	TTAR-01.0021, 머신러닝 기반 양자암호 분배 네트워크 (QKDN) 상호운용 (Interworking) 제어 및 관리를 위한 유스케이스(기술보고서)	2021
	TTAR-01-0022, 양자 암호 네트워크의 유스케이스(기술보고서)	2021
	TTAK.KO-01.0230, 양자 키 분배(QKD) 용어 정의	2021
	TTAK.KO-01.0214/R1, 양자암호 전달 네트워크의 기능구조	2021
	TTAK.KO-01.0225/R1, QKD 네트워크 (QKDN); QKD 시스템과 양자 암호키 관리 시스템간 인터페이스 및 YANG 데이터 모델	2021
	TTAE.IT-Y.3800, 양자키 분배망 개요	2020
	TTAE.ET-GS QKD 011, 양자 키 분배(QKD): 구성 요소 특성화: QKD 시스템의 광학 구성 요소 특성화	2018
	TTAE.ET-GS QKD 008, 양자 키 분배(QKD): 모듈 보안 규격	2018
	TTAE.ET-GS QKD 003, 양자 키 분배: 구성 요소 및 내부 인터페이스	2017
	TTAE.ET-GS QKD 004, 양자키 분배망: 응용 인터페이스	2017
TTA PG501	TTAK.KO-12.0329-Part1, 양자 키 분배 – 제1부: 일반	2018
	TTAK.KO-12.0329-Part2, 양자 키 분배 – 제2부: BB84 프로토콜	2018
TTA PG503	2019-1114, IP 보안프로토콜(IPsec)과 양자 암호 키 분배 장비간 연동 규격	진행중 (2023)
TTA PG504	TTAK.KO-12.0356, 양자키분배 보안 요구사항	2019

2.4.2. 국제 표준화 현황 및 전망

o 공식 표준화 기구

- ITU-T SG11
  - 신호 방식을 위한 프로토콜 구조 및 응용제어, 세션 및 접속제어, 신호처리, 적합성 및 상호 운용성 시험 분야의 표준 개발 중
  - 양자키분배망의 각 인터페이스별 세부 프로토콜을 정의하고 있으며, 현재 5개의 표준을 개발하고 있음
- ITU-T SG13
  - ITU-T SG13은 미래 통신망(Future Networks) 분야 표준화를 담당하는 그룹으로 IMT-2020 and beyond (5G 및 6G), 클라우드와 빅데이터, 신뢰 네트워크와 양자암호 네트워크 표준 개발 중
  - KT가 '21년말 제안한 미래양자 통신망(QEFN: Quantum Enabled Future Network) 주제로 양자인터넷 표준 개발 착수 함
- ITU-T SG17
  - ITU-T에서 '보안' 영역 표준화를 담당하는 그룹으로 Question 15에서 QKD 및 QRNG 보안 전반에 대한 표준 개발 중
  - QKD 네트워크 보안 요구사항, 키 관리 보안 요구사항 등의 표준화, QRNG 구조, QKD 키와 암호키를 결합하는 등의 하이브리드 키 교환 등에 대한 표준화를 완료하였으며 현재는 QKD 네트워크 내부 인증 및 허가, 관리 기능 등의 영역의 보안 요구사항과 신뢰노드에 대한 보안 요구사항 표준화가 진행 중에 있음
- ITU-T TSAG
  - TSAG(Telecommunication Standardization Advisory Group)은 ITU-T의 조직과 활동에 대한 자문그룹으로, 연구 그룹 간 혹은 타 SDO와의 협력을 총괄 담당함.
  - TSAG은 기술표준 개발을 직접 수행하지는 않으나, 연구 그룹 간 공동 활동이 필요한 Focus Group 설립·운용 시 이를 산하에 배치하고 있음.
  - 양자네트워크 관련된 활동으로는 지난 '19년 한국 KT가 중국 산업계와 공동으로 신규설립을 제안한 ITU-T Focus Group on QIT4N(Quantum Information Technology for Networks)의 상위그룹 역할을 수행했음.
    * 2021년 활동을 종료한 본 FG는 QIN(Quantum Information Network) 표준화 요소를 검토하고, 양자기기(양자컴퓨터, 양자센서, 양자시계, 양자암호시스템 등)를 네트워크화하기 위한 후속 표준화를 제안했음.

- JTC1 SC27
  - 정보보호, 사이버보안, 개인정보보호를 목적으로 하는 표준을 개발하는 그룹으로, 정보 및 ICT 보안 관리, 정보 암호화 및 기타 보안 메커니즘, 보안 관리 지침, 신원 관리, 정보보안 시스템 적합성 평가 및 평가 방법론 등의 표준들을 개발하고 있음
  - JTC1 SC27 산하 WG3(보안평가 방법, 테스트 방법 및 명세서 정의를 위한 그룹)에서 CC를 기반으로 양자키분배 장치의 보안 요구사항과 시험 방법 두 개의 표준을 진행 중이며, 현재 DIS(Draft International Standard) 단계에 있음 (ISO/IEC 23837). 최근 해당 표준에 대해 ETSI가 PP를 구성하여 제안함
- JTC1 WG14
  - 양자 컴퓨팅 표준화를 위해 설립되었으며, 양자 컴퓨팅 연구개발 과정에서 다양하게 발생하고 있는 격차와 기회를 확인하고, 이를 해소할 수 있는 결과물을 개발하는 것을 목표로 함
  - 양자 컴퓨팅 세부 기술에 대한 초기화에 앞서 양자 컴퓨팅 용어 정의에 관한 표준화 작업이 먼저 진행 중

< 국제 표준화 현황 >

표준화기구	표준(안)명	완료연도
JTC1 SC27	ISO/IEC 23837-1, Information technology security techniques - Security requirements, test and evaluation methods for quantum key distribution - Part 12: Requirements	진행중 (2023)
	ISO/IEC 23837-2, Information technology security techniques - Security requirements, test and evaluation methods for quantum key distribution - Part 2: Evaluation and testing methods	진행중 (2023)
JTC1 WG14	ISO/IEC CD 4879, Quantum computing – Terminology and vocabulary	진행중 (2023)
ITU-T SG11	Q.QKDN_profr, Quantum key distribution networks – Protocol framework	2022
	Q.QKDN_Ak, Protocols for Ak interface for QKDN	2022
	Q.QKDN_Ck, Protocols for Ck interface for QKDN	2022
	Q.QKDN_Kq-1, Protocols for Kq-1 interface for QKDN	2022
	Q.QKDN_Kx, Protocols for Kx interface for QKDN	2022

표준화기구	표준(안)명	완료연도
ITU-T SG13	Y.QKDN-qos-iw-req, Requirements of QoS assurance for QKDN interworking	2023
	Y.QKDN-qos-mmq, Quantum key distribution Networks – Measurement methodology for QoS parameters	2023
	Y.QKDN-iwac, Quantum key distribution networks interworking - architecture	2023
	Y.QKDNf-fr, Framework of Quantum Key Distribution Network Federation	2023
	Y.QKDNi-SDNC, Quantum Key Distribution Network Interworking - Software Defined Networking Control	2023
	Y.supp.QKDN-roadmap, Standardization roadmap on Quantum Key Distribution Networks	2023
	Y.3807, Quantum key distribution networks – Quality of service parameters	2022
	Y.3808, Framework for integration of quantum key distribution network and secure storage network	2022
	Y.3809, A role-based model in quantum key distribution networks deployment	2022
	Y.3810, Quantum key distribution network interworking-framework	2022
	Y.3811, Quantum key distribution network – Functional architecture for quality of service assurance	2022
	Y.3812, Quantum key distribution network – Requirements for machine learning based quality of service assurance	2022
	Y.QKDN-iwrq, Quantum key distribution networks interworking - functional requirements	2022
	Y.QKDN-ml-fra, Quantum key distribution networks - functional requirements and architecture to enable machine learning	2022
	Y.QKDN-rsfr, Framework of quantum key distribution network resilience	2022
	Y.TR-QEFN, ITU-T's Views for Quantum-Enabled Future Networks	2022
	Y.3805, Quantum key distribution networks – Software-defined networking control	2021
	Y.3806, Quantum key distribution networks – Requirements for quality of service assurance	2021
	Y.3801, Functional requirements for quantum key distribution networks	2020
	Y.3802, Quantum key distribution networks – Functional architecture	2020
	Y.3803, Quantum key distribution networks – Key management	2020
	Y.3804, Quantum key distribution networks – Control and management	2020
	Y.3800, Overview on networks supporting quantum key distribution	2019

표준화기구	표준(안)명	완료연도
ITU-T SG17	X.sec_QKDN_AA, Authentication and authorization in QKDN using quantum safe cryptography	진행중 (2023)
	X.sec_QKDN_CM, Security requirements and measures for quantum key distribution networks – control and management	진행중 (2023)
	X.sec_QKDN_tn, Security requirements and designs for quantum key distribution networks – trusted node	진행중 (2023)
	TR.hyb-qkd, Overview of hybrid approaches for key exchange with QKD	2022
	X.1710, Security framework for quantum key distribution networks	2021
	X.1712, Security requirements and measures for QKD networks – key management	2021
	X.1714, Key combination and confidential key supply for quantum key distribution networks	2021
	X.STR.SEC-QKD, Security considerations for quantum key distribution network	2020
	X.1702, Quantum noise random number generator architecture	2020
ITU-T FG-QIT4N	Quantum information technology for networks terminology: Network aspects of quantum information technologies	2021
	Quantum information technology for networks use cases: Network aspects of quantum information technologies	2021
	Standardization outlook and technology maturity: Network aspects of quantum information technologies	2021
	Quantum information technology for networks terminology: QKDN	2021
	Quantum information technology for networks use cases: QKDN	2021
	Quantum key distribution network protocols: Quantum layer	2021
	Quantum key distribution network protocols: Key management layer, QKDN control layer and QKDN management layer	2021
	Quantum key distribution network transport technologies	2021
	Standardization outlook and technology maturity: Quantum key distribution network	2021

o 사실 표준화 기구

- ETSI ISG QKD
  - 2008년에 창설되어 대부분 유럽에 기반을 둔 QKD 제조사, 통신사업자, 대학과 연구기관들이 참여함
  - 해당 그룹에서 QKD에 대해 20개가 넘는 산업 규격 문서를 발간함. 단, ETSI의 정식 표준은 아님
- IEEE QCN-WG
  - QCN-WG는 Quantum Computing Nomenclature Working Group으로 향후 양자컴퓨팅 관련 기술 표준 및 산업 솔루션 개발에서 사람들이 함께 일할 수 있는 전 세계적으로 개방된 합의 구축환경 및 플랫폼을 제공하고자 함
  - 양자컴퓨팅 용어, 성능 지표 및 벤치마크, 시스템 아키텍쳐, 알고리즘 개발, 시뮬레이터 등에 관한 표준화 작업 진행(P7130)
- IRTF QIRG
  - IRTF는 IETF와 형제기구로, IETF는 인터넷 관련 엔지니어링과 표준화에 집중하고 있음을 감안할 때, IRTF는 상대적으로 장기간이 예상되는 연구주제에 집중하고 있음
  - 산하 QIRG(Quantum Internet Research Group)은 양자 인터넷 표준화를 위한 연구 및 선행 표준 개발 진행중
  - 2019년 3월에 개발을 시작한 양자 인터넷 구조원리(Architecture Principle for a Quantum Internet)와 응용시나리오(Application Scenarios for the Quantum Internet)가 있으며, 양자인터넷 표준화 이전에 양자물리학을 포함한 기초기술에 대한 이해와 공유를 목표로 하고 있음

< 국제 표준화 현황 >

표준화기구	표준(안)명	완료연도
ETSI ISG QKD	GS QKD 018, Quantum Key Distribution; Ochestration Interface for Software Defined Networks	2022
	GS QKD 015, Quantum Key Distribution; Control Interface for Software Defined Networks	2022
	GS QKD 004, Quantum Key Distribution; Application Interface	2020
	GS QKD 014, Quantum Key Distribution; Protocol and data format of REST-based key delivery API	2019
	GS QKD 012, Quantum Key Distribution; Device and Communication Channel Parameters for QKD Deployment	2019
	GR QKD 007, Quantum Key Distribution; Vocabulary	2018

표준화기구	표준(안)명	완료연도
ETSI ISG QKD	GS QKD 003, Quantum Key Distribution; Components and Internal Interfaces	2018
	GS QKD 011, Quantum Key Distribution; Component Characterization: Characterizing optical components for QKD systems	2016
IEEE	IEEE P7130, Standard for Quantum Technologies Definitions	진행중 (2023)
IRTF QIRG	Draft-irtf-qirg-principles, Architectural Principles for a Quantum Internet	진행중 (2023)
	Draft-irtf-qirg-internet-use-cases, Application Scenarios for the Quantum Internet	2022

양자정보통신

ICT Standardization Strategy Map

Part

Ⅲ

국내외 표준화 추진전략

Ⅲ. 국내외 표준화 추진전략

3.1. 표준화 SWOT 분석

<table>
<tr><th colspan="3" rowspan="2">국내역량요인 / 국외환경요인</th><th colspan="2">강 점 요 인 (S)</th><th colspan="2">약 점 요 인 (W)</th></tr>
<tr><td>시장</td><td>- 정부·공공 망사업에 양자키분배 장비 도입 증가
- KT, SKT 등 망사업자들의 적극적으로 개발에 투자</td><td>시장</td><td>- 기술의 고비용으로 인하여 보편적 보급에는 한계
- 신규 시장 형성을 위한 기술 성숙도는 부족</td></tr>
<tr><td colspan="3"></td><td>기술</td><td>- 양자정보통신이 10대 국가필수 전략기술에 포함
- 정부의 지원확대로 다양한 원천 기술 확보 추진 중</td><td>기술</td><td>- 핵심원천기술 확보 수준 미흡
- 양자분야의 고급 개발 인력 부족</td></tr>
<tr><td colspan="3"></td><td>표준</td><td>- 양자키분배 및 네트워크에 대한 국제표준화 기여도 높음
- 국내 및 국제표준화 경험을 토대로 신규 표준화 활동 용이</td><td>표준</td><td>- 국제 표준화 주도 전문가 부족
- 기술개발 중심으로 표준화 추진 환경 미성숙</td></tr>
<tr><td rowspan="3">기회요인 (O)</td><td>시장</td><td>- 양자정보통신기술은 미래 산업·안보의 게임체인저로 부상
- 양자기술을 다양한 분야를 적용하기 위한 상용화 활발</td><td colspan="2" rowspan="3">【SO전략】

- (시장) 양자키분배 및 네트워크 분야의 상용화 경험을 살려, 국내외 시장 진출
- (기술) 상용화에 필요한 핵심기술에 대한 원천기술 확보
- (표준) ITU-T, IEC, JTC1에서 활동 중인 전문가를 활용한 다양한 국제기구에서 리더십 확보</td><td colspan="2" rowspan="3">【WO전략】

- (시장) 기 확보한 기술을 활용한 서비스 시장 개척
- (기술) 국제 경쟁력을 확보할 수 있는 방향을 선정하여 투자
- (표준) 국제표준화에 활용할 수 있는 다양한 표준에 대한 선행연구 및 전략 수립</td></tr>
<tr><td>기술</td><td>- 양자정보통신분야 국가경쟁력 확보를 위하여 대규모 투자
- 상용화를 위한 필요기술에 연구 및 ICT 적용 확대</td></tr>
<tr><td>표준</td><td>- ITU-T, IEC, JTC1 등에서 양자 분야 표준화 움직임 활발
- 표준화 초기 단계로 상용화를 위한 다수의 표준화 필요</td></tr>
<tr><td rowspan="3">위협요인 (T)</td><td>시장</td><td>- 소수 글로벌 기업의 시장 독점 우려
- 외국 기업들의 핵심원천 기술 선점</td><td colspan="2" rowspan="3">【ST전략】

- (시장) 국내 환경 선적용을 통해 제품 인지도와 완성도를 제고하여 해외 시장 경쟁력 확보
- (기술) 핵심 기술 개발 및 표준화의 종합적인 로드맵 마련과 체계적인 국가 R&D 프로젝트 추진
- (표준) 국제표준화 주도를 통한 표준 IPR 확보로 외국 기업의 특허 공격으로부터 국내 산업 보호</td><td colspan="2" rowspan="3">【WT전략】

- (시장) 국내 산·학·연 연계를 통한 기술 개발 및 활용의 선순환 체계 구축
- (기술) 특화된 핵심원천 기술의 장기적인 R&D 진행 및 국외 R&D 공동연구, 핵심부품에 대한 중장기적 확보 노력
- (표준) 양자를 활용하는 보안, ICT 분야의 표준전문가들과 협력체계 마련</td></tr>
<tr><td>기술</td><td>- 국가 차원의 원천기술 확보 경쟁 심화
- 중국의 양자정보통신기술 수준 급상승</td></tr>
<tr><td>표준</td><td>- 보안관련 표준화에는 보안 그룹과의 협력 필요</td></tr>
<tr><td colspan="7">표준화 추진상의 문제점 및 현안 사항</td></tr>
<tr><td colspan="7">- 양자정보통신분야는 표준화 초기 단계로, 표준화 추진에 대한 전반적인 체계와 전문가 부족</td></tr>
</table>

3.2. 중점 표준화 항목

o 표준화 항목 중분류 범위의 설정

- 양자정보통신 기술은 양자의 양자역학적 특성(중첩, 얽힘, 비가역성, 불확정성)을 정보통신에 적용하기 위한 기술로, 양자의 도청 불가능성을 이용한 암호키를 분배하기 위한 규격·시스템·네트워크 등의 양자암호통신, 양자의 중첩된 데이터의 병렬적 처리 기능을 이용하기 위한 아키텍쳐·시뮬레이션·알고리즘 등의 양자 컴퓨팅, 양자의 분해능, 민감도를 이용한 관성·시간측정·자기장·전기장·광학 센서 등의 양자센싱, 양자 디바이스들을 연결하기 위한 양자네트워크 분야별로 개발하고 있으며, 본 ICT 표준화 전략의 양자정보통신 분과의 중분류 범위는 양자정보통신 분야의 주요 표준화 기구 작업 그룹별 표준화 범위와 시스템을 구성하는 필수 단위 기술을 중심으로 구분

< 양자정보통신 Ver.2023 표준화 항목 >

표준화 항목		표준화 내용	Target SDOs	표준화 특성	중점 항목
양자 암호통신	양자키분배 규격 및 시험 표준	QKD의 기본 원리 및 안전성 평가에 대한 표준 - QKD 프로토콜 표준 - QKD 후처리 프로토콜 및 기술 표준 - QKD 보안 평가 및 시험 표준	ITU-T SG17, JTC1 SC27 WG3, ETSI ISG QKD	⑤	O
	양자키분배 시스템 표준	QKD 시스템 구성 및 네트워크 연계를 위한 표준 - QKD 시스템의 구성요소 구현 표준 - QKD 인터페이스 및 구조 표준 - QKD 요소기술 규격 표준 - QKD 시스템의 제어 표준 - 인공지능 연계 양자키분배 시스템 표준 - 스마트 양자키분배 시스템 아키텍처 표준	ETSI QKD/ QSC, ITU-T SG13/ SG17, IETF	⑤	O
	양자키분배 프로토콜 및 키관리 표준	양자 암호 통신망의 프로토콜과 키관리 보안성 확보와 검증을 위한 표준 - QKD 통신망의 프로토콜 표준, QKD 및 키관리 시스템 구성 표준 - 하이브리드 암호 키 생성 표준 - 노드 간 양자암호키 전달을 위한 구조 표준, QKD 신뢰노드 요구사항 표준	ETSI ISG QKD, ITU-T SG11/ SG13/ SG17	①,②, ⑤	O

표준화 항목		표준화 내용	Target SDOs	표준화 특성	중점 항목
양자 암호통신	양자키분배 네트워크 및 망관리 표준	QKD 네트워크와 망관리 및 스마트 양자 보안시스템 아키텍처 표준 - QKD 네트워킹 기술 및 네트워크 토폴로지 표준 - QKD 네트워크 망관리와 제어 표준 - QKD 이기종 네트워크 간 연동 표준 - SDN/광전송 연동 인터페이스 및 구조 표준 - 인공지능 연계 양자 보안 시스템 표준 - 스마트 양자 보안시스템 아키텍처 표준	ITU-T SG11/ SG13/ SG17, ETSI ISG QKD	①,③	O
	양자 서명 및 인증 표준	양자서명/양자인증 관련 표준 - 양자서명/양자인증 프로토콜 표준 - 양자서명/양자인증 오류 정정 및 후처리 기술 표준 - 양자서명/양자인증 보안성 평가 및 시험 방법 표준	JTC1 SC27, ETSI ISG QKD, ITU-T SG17	①,③,⑤	X
	양자 난수발생기 표준	양자 난수발생기 구조 및 활용에 대한 표준 - 양자난수발생기 원리 및 기술 표준 - 양자난수발생기 보안 규격 표준 - 양자난수발생기 활용에 따른 요구사항 표준	ETSI ISG QKD, ITU-T SG17	⑤	X
양자 컴퓨팅	양자컴퓨터 아키텍쳐 표준	양자컴퓨터의 기술적 구성 및 성능평가 지표에 관한 표준 - 양자 컴퓨터 구성 - 양자컴퓨터의 하드웨어 및 시스템 소프트웨어 구성요소 - 양자컴퓨터 하드웨어 및 소프트웨어의 성능 기준	IEEE P3120, IEEE P7131	③,④,⑤	X
	양자 알고리즘 표준	양자 알고리즘 설계 방법에 관한 표준 - 양자 우월성에 기반한 양자 알고리즘의 기계적 설계 방안 (프로그래밍 기술은 제외)	IEEE P2995	③,④,⑤	X
	양자 시뮬레이션 표준	양자 시뮬레이터 디바이스 타입에 따라 양자현상 모사를 프로그래밍하는 방법에 관한 표준 - 양자 시뮬레이터 (아날로그, 디지털, 하이브리드) 에 대한 프로그래밍 방법 (양자 시뮬레이션 장치의 나노 스케일 속성을 표현/조작하기 위한 알고리즘)	IEEE P3155	③,④,⑤	X
	양자 컴퓨팅 용어 표준	양자컴퓨팅 관련 용어에 대한 표준 - 양자정보기술 구현에 필요한 양자역학 용어 - 양자컴퓨팅 소프트웨어 관련 용어 - 양자컴퓨팅 하드웨어 관련 용어	JTC1 WG14, IEEE QCN-WG	①	O

표준화 항목		표준화 내용	Target SDOs	표준화 특성	중점 항목
양자 센싱	관성 센서 표준	양자센싱 관련 관성 센서 표준 - 관성 센서 성능평가 항목, 평가방법, 평가기술 등 - 측정 물리량: 중력, 가속도, 회전속도 등	-	①	X
	시간측정 센서 표준	양자센싱 관련 시간측정 센서 표준 - 시간 및 주파수 발생기 및 측정기 성능평가 항목, 평가방법, 평가기술 등 - 측정 물리량: 시간간격, 주파수, 시각동기화 정도 등	-	①	X
	자기장·전기장 센서 표준	양자센싱 관련 자기장·전기장 센서 표준 - 자기장 센서, 전기장 센서 성능평가 항목, 평가방법, 평가기술 등 - 측정 물리량: 자기장 세기(ac, dc), 전기장 세기, 이미지 분해능, 주파수 등	-	①	X
	광학 센서 표준	양자센싱 관련 광학센서 표준 - 광학 센서 성능평가 항목, 평가방법, 평가기술 등 - 측정 물리량: 변위, 이미지 분해능, 파장대역, 측정감도 등	-	①	X
양자 네트워크	양자 네트워크 구조 표준	양자 네트워크의 구조 관련 표준 - 일반 구조(General Architecture), 계층 모델(Layered Model) 기술 - 계층별 기능/기술 요구사항(Functional & Technical Requirements) 등	ITU-T SG13, IRTF	②, ③, ④	O
	양자 전송 기술 표준	양자 전송기술에 대한 표준 - 전송 프로토콜 - 전송 오류 정정 - 양자 중계(ex, 얽힘, 양자 메모리 등) - 양자 디바이스 연동 - 양자 전송 성능 기준 및 평가	ITU-T SG11/ SG13	①,②,③	X
	양자 네트워킹 기술 표준	양자 네트워킹 기술에 대한 표준 - 양자 스위칭/라우팅 구조 및 프로토콜, 주소체계, Legacy 네트워크 연동, 사업자간/국가간 연동 등	ITU-T SG11/ SG13	⑤	X
	양자 네트워크 제어 및 관리 기술 표준	양자 네트워크 제어 및 관리 기술에 대한 표준 - 제어 및 관리 구조, 신호(Signaling) 프로토콜, 최적 경로제어(QoS, Shortest, availability등) - 구성/성능/장애 관리, 제언/관리 인터페이스 등	ITU-T SG11/ SG13	⑤	X
	양자 네트워크 서비스 표준	양자 네트워크 서비스에 대한 표준 - 양자키분배 (QKD), 분산형 양자컴퓨팅 (Distributed Quantum Computing) - 양자 센서 네트워크(Quantum Sensing Network)	ITU-T SG11/ SG13	①,②,③	X

< 표준화 특성 >

① : 개념, 정의 표준　② : 유즈케이스, 요구사항 표준　③ : 기능 도출, 참조구조 표준
④ : 데이터포맷, 스키마 표준　⑤ : 프로토콜, 인터페이스 표준　⑥ : 시험, 가이드라인 표준

o 추진경과

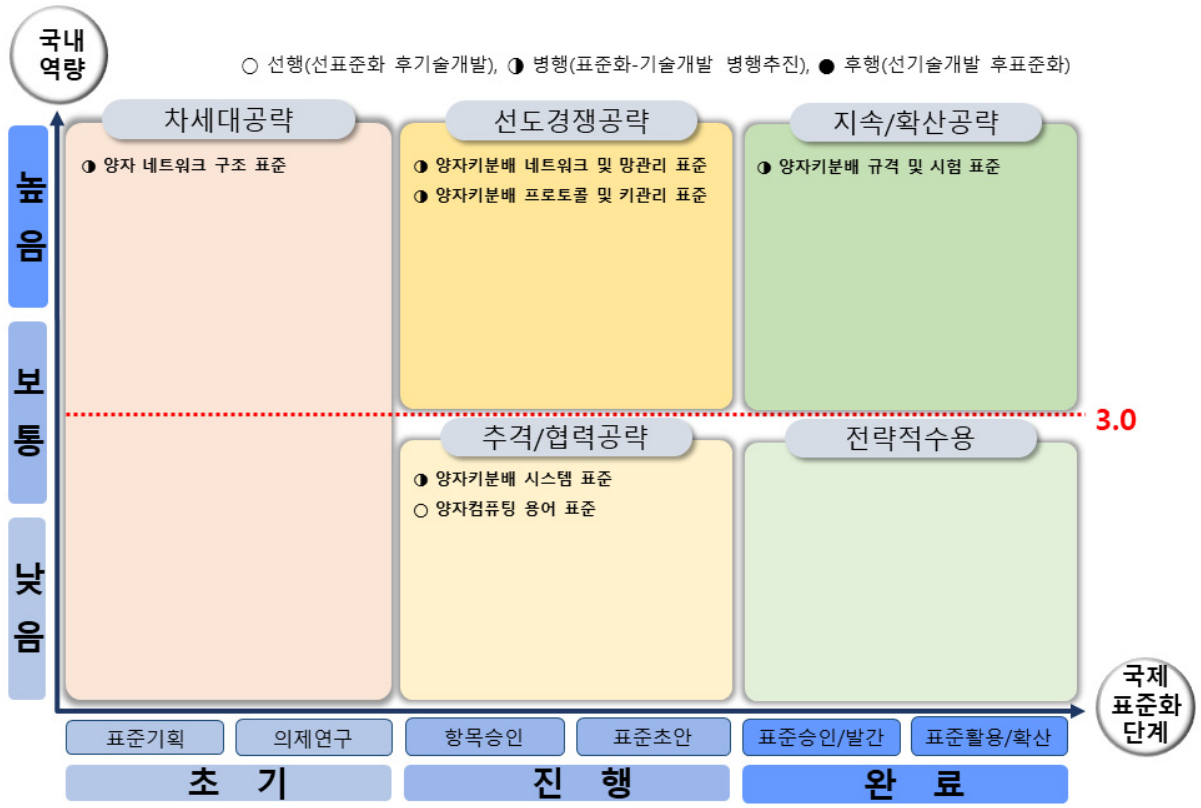
- Ver.2023(2022년)에서는 양자정보통신 분과가 신설됨에 따라 Ver.2022의 차세대 보안과 지능형 네트워크 분과에서 진행되었던 양자암호통신 관련 중점항목들을 이관받아 양자키분배 규격 및 시험표준, 양자키분배 시스템 표준, 양자키분배 신뢰노드 및 키관리 표준, 양자키분배 네트워크 및 망관리 표준으로 재편하였으며, 표준화 진행이 초기 단계인 양자 컴퓨팅은 용어 표준만을 중점항목으로 선정하였고, 양자 센싱은 표준화가 진행되지 않아 중점항목을 선정하지 않았으며, 양자 네트워크에서는 ITU-T에서 표준화가 시작되는 양자 네트워크 구조 표준을 중점항목으로 선정

< 버전별 중점 표준화 항목 비교표(3개년) >

* Ver.2023 신규항목

구분	Ver.2021	Ver.2022	Ver.2023
양자암호통신	양자 암호기술 표준 (차세대 보안)	양자 암호기술 표준 (차세대 보안)	양자 키분배 규격 및 시험 표준*
	양자 정보통신 시험 및 인증 표준 (지능형 네트워크)	양자 정보통신 시험 및 인증 표준 (지능형 네트워크)	양자 키분배 시스템 표준*
	-	-	양자 키분배 프로토콜 및 키관리 표준*
	양자암호 통신망 표준 (지능형 네트워크)	양자암호 통신망 표준 (지능형 네트워크)	양자 키분배 네트워크 및 망관리 표준*
양자컴퓨팅	-	-	양자 컴퓨팅 용어 표준*
양자 센싱	-	-	-
양자네트워크	-	-	양자 네트워크 구조 표준*

3.3. 중점 표준화 항목별 추진전략



○ 영역별 특징 및 대응전략

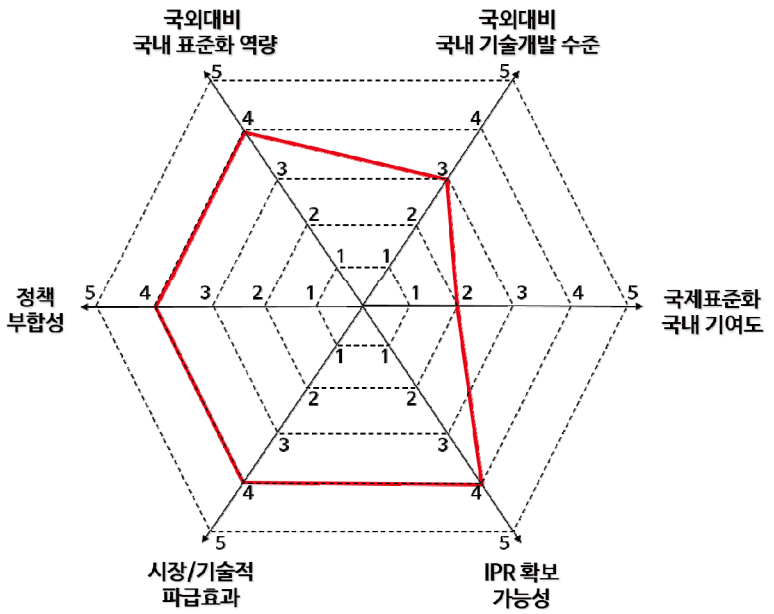
- **차세대공략** : 미래 핵심기술 및 유망서비스 신규 표준 제안을 통해 표준화를 선점할 수 있는 분야
  : 국제표준 기획 단계부터 주도적 참여를 통해 국제표준화 선도 기반 확보
  : 관련 표준화기구에서의 적극적인 제안으로 국내 핵심 기술의 국제표준화를 위한 발판 마련

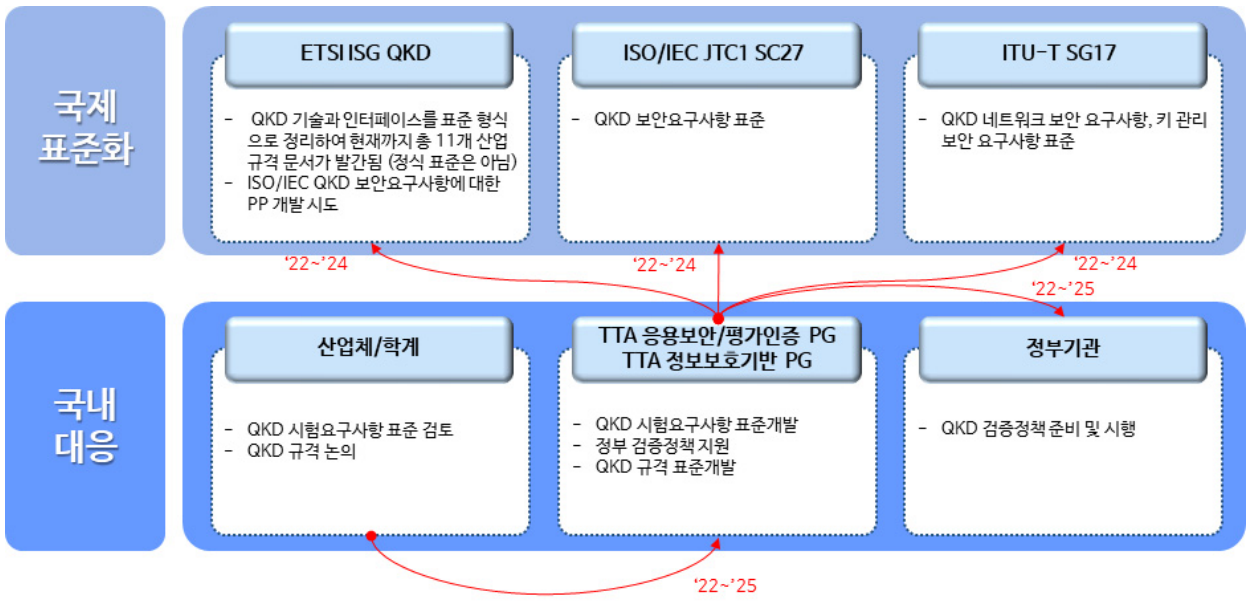
- **선도경쟁공략** : 표준화 경쟁이 치열하지만 국내역량이 높아 국제표준 선도가 가능한 분야
  : 국내 기술의 국제표준 반영을 위한 관련 표준화기구에서의 적극적인 표준화활동 추진

- **추격/협력공략** : 국제표준화가 활발히 진행 중인 분야 중 국내 진입시기가 다소 늦어졌지만 타 국가의 표준화 수준에 도달하기 위해 후발주자로써 추격하거나 다각화된 협력이 필요한 분야
  : 국제 공식 및 사실표준화기구, 포럼, 컨소시엄에서의 다각적인 대응 방안 모색
  : 전략적 대외협력 강화 및 제휴를 통한 기술/표준의 Catch-up 전략 추진

- **지속/확산공략** : 국제표준화가 거의 완료단계이나 국내역량이 높아 후속/개정 표준화에서의 선도가 예상되며, 표준 기반 서비스 및 시장 확산에 집중이 필요한 분야
  : 높은 국내 역량을 바탕으로 한 후속/개정 표준화 주도 및 추가적인 틈새표준 발굴을 모색
  : 표준기반 킬러 애플리케이션 개발 및 서비스 적용을 통한 표준 활용 촉진

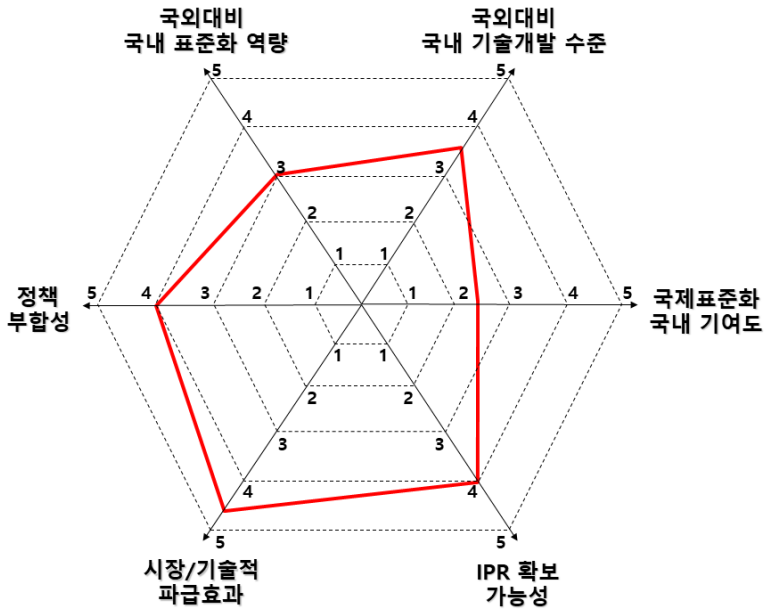
- **전략적수용** : 국제표준화가 거의 완료된 분야 중 국내역량은 낮지만 전략적으로 수용이 필요한 분야
  : 국제표준의 수용 및 적용을 통한 국제 호환성 확보와 국내 시장 확산

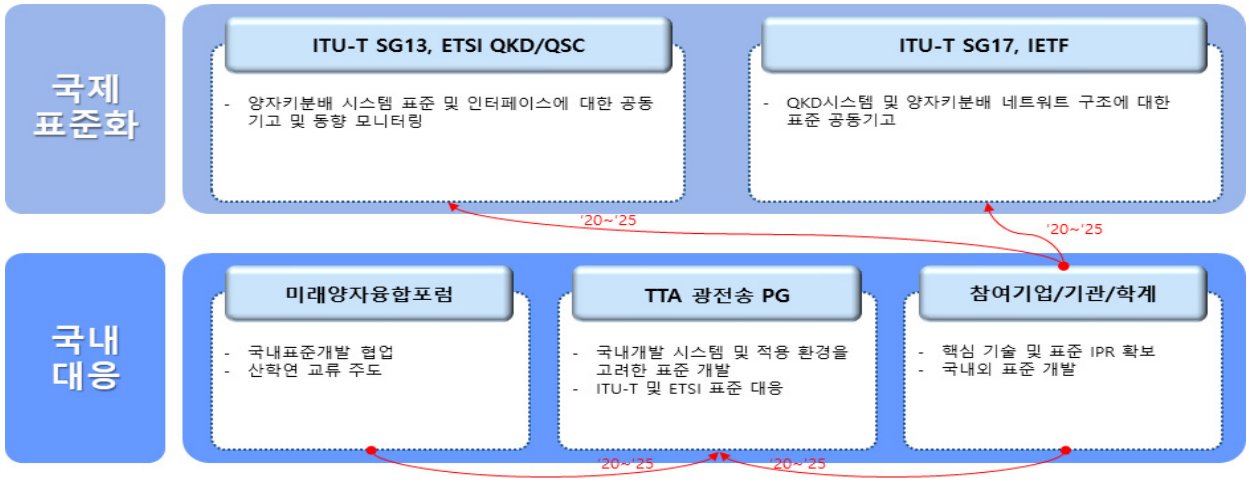
<table>
<tr><th colspan="6">(지속/확산공략 | 병행) 양자키분배 규격 및 시험 표준</th></tr>
<tr><td>주요 내용</td><td colspan="5">ㅇ 양자키분배를 구현하는데 필요한 공통 규격 표준과 양자키분배 시스템을 시장에 도입하기 위한 안전성 평가 시험 표준 개발
- 양자키분배를 구현하는데 필요한 규격 도출 및 표준 개발
- 양자키분배의 안전성을 시험하기 위한 요구사항과 절차 표준</td></tr>
<tr><td>필요성</td><td colspan="5">ㅇ 양자키분배 기술의 성공적인 상용화를 뒷받침할 기술 규격과 평가인증의 제도적 정착에 필요한 표준이 필요함
- 양자키분배가 상용화되어 있으므로 양자키분배 기술 규격에 대한 표준이 산·학·연의 협조 아래 시급히 추진되어야 함
- 평가인증과 관련된 표준이 국내표준으로 이미 채택되었으나 후속 표준의 신규 진행이 필요함</td></tr>
<tr><td>전략적 중요도 / 국내 역량</td><td colspan="2"> 
</td><td>표준화 기구/ 단체</td><td>국내</td><td>TTA 응용보안/평가인증 PG, TTA 정보보호 기반 PG</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td>국제</td><td>ITU-T SG17, JTC1 SC27, ETSI ISG QKD</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td>국내 참여 업체/ 기관</td><td>ETRI, KT, SKT</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="4">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td></tr>
<tr><td>국외</td><td colspan="4">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td></tr>
<tr><td>선도국가/기업</td><td colspan="2">(미국) MagiQ, (유럽) Toshiba EU, (스위스) IDQ</td><td>기술 수준</td><td>80%
(선도국가대비)</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="4">□표준기획↦□의제연구↦□항목승인↦■표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>국제</td><td colspan="4">□표준기획↦□의제연구↦□항목승인↦□표준초안↦■표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>선도국가/기업</td><td colspan="2">(중국) CESI, (유럽) Toshiba EU</td><td>표준 수준</td><td>90%
(선도국가대비)</td></tr>
<tr><td colspan="6">- Trace Tracking : 지속/확산공략(Ver.2023 신규)
ETSI에서 산업 규격으로 QKD 기술 전반의 기술이 정리됨. ISO/IEC JTC1 SC27에서는 기존 IT 제품에 대한 보안평가 인증에 사용되는 공통평가기준(CC, Common Criteria)을 기반으로 QKD의 안전성을 평가하기 위한 보안 요구사항과 시험 방법 표준이 진행되어 현재 DIS 단계에 있음. QKD 규격에 대한 정식 표준은 없지만 선행되는 QKD 관련 기본 표준들이 최종 단계에 이른 만큼 미흡한 표준에 대한 논의와 개발이 이루어질 것으로 예상되어 지속/확산공략 항목으로 분류함</td></tr>
</table>



< 국제표준화 대응체계 >

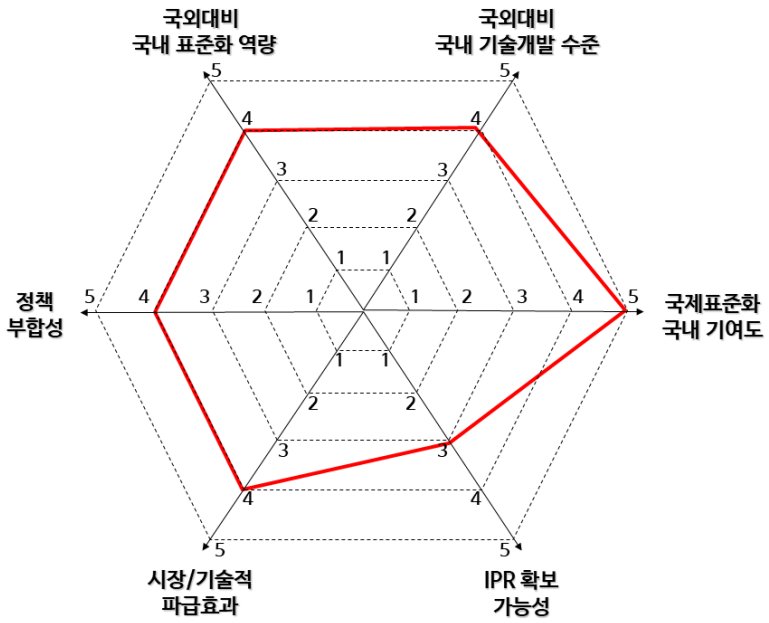
국제 표준화 추진 전략	**<표준화 계획>** - 현재 ISO/IEC에서 QKD 안전성 보안 요구사항에 대한 표준이 DIS 단계에 이르러 곧 정식 표준으로 확정될 예정임. 단, 해당 표준의 대상이 되는 프로토콜 표준은 없음 - ETSI에서 양자키분배 관련 산업 규격에 대한 연구 및 출간물은 있으나 ETSI의 정식 표준은 아님. 양자키분배 규격 표준에 대한 계획 없음 **<대응방안>** - (공식표준화 대응전략: 국제표준화기구 활동(적극대응)) QKD 프로토콜에 대한 표준이 없으므로 국내 표준기구를 통한 QKD 프로토콜들을 선 표준화한 뒤 국제 표준기구에서 해당 분야의 표준화 추진
국내 표준화 추진 전략	**<표준화 계획>** - TTAK.KO-12.0356(양자 키 분배 보안 요구사항)의 후속으로 시험 요구사항 표준 추진 - QKD의 다양한 프로토콜 중 산업적으로 활용 가능한 프로토콜을 선택하여 표준 추진 - QKD 공통 규격 표준 추진 **<대응방안>** - (표준화위원회 PG 활동/연구개발 표준화 연계 개발) 2023년에 시행 예정인 QKD 장비의 적합성 검증 체계와 연동하여 TTA, ETRI 등의 시험기관의 협조 아래 QKD 보안 요구사항의 고도화 및 시험 요구사항 개발
표준특허 전략	- **(표준 및 R&D 중후기 전략 : 특허 권리범위 보완전략)** 국내에서 2023년 시행될 QKD 안전성 검증정책에서 파생되는 기술을 특허 및 국내표준으로 확보하고 국제 표준 및 특허에 적극 대응. QKD 규격을 국내에서 선행 표준화하여 국제 표준 선도 역할 확보
중단기 전략 (3개년)	

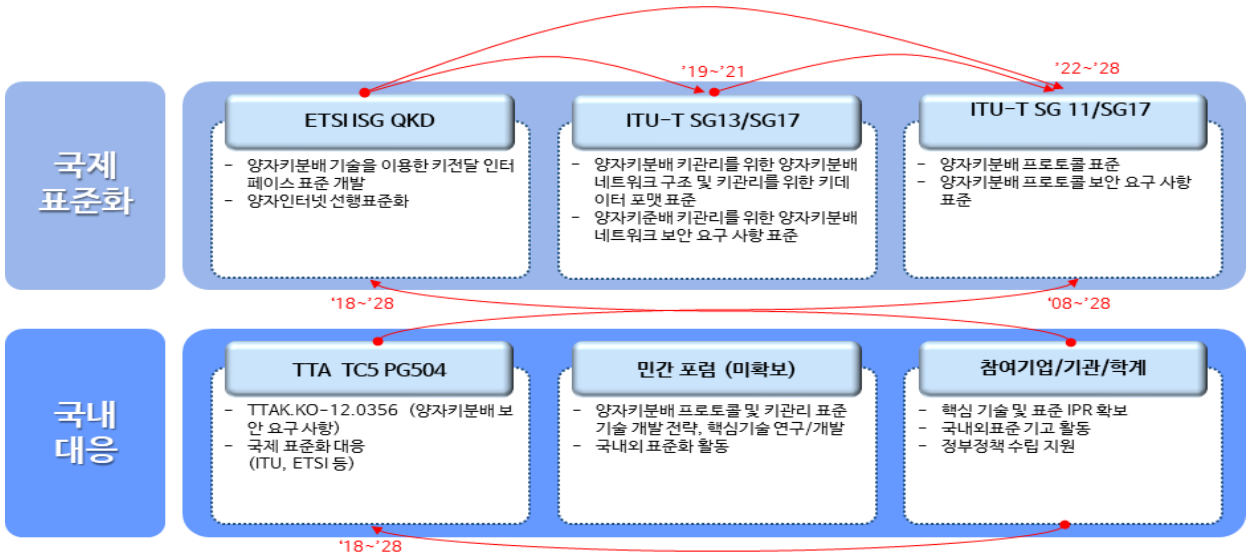
<table>
<tr><th colspan="6">(추격/협력공략 | 병행) 양자키분배 시스템 표준</th></tr>
<tr><td>주요 내용</td><td colspan="5">○ 양자키분배 시스템 개발에 광학계를 비롯한 구성요소 표준, 구성요소들의 제어에 대한 표준, 네트워크 연계를 위한 인터페이스 표준, 인공지능 등을 활용하기 위한 표준 개발</td></tr>
<tr><td>필요성</td><td colspan="5">○ 양자키분배 시스템은 광학계 및 이를 제어하는 요소들이 안전성을 위배하지 않도록 구현되는 게 필요하며, 양자키분배 시스템은 네트워크와 연계하여 동작하므로 네트워크 인터페이스 규격이 필요
- 다양한 양자키분배 장치가 개발되고 있어, 구현에 따른 안전성 확보를 위해서는 이에 대한 표준화 시급
- 개발된 표준은 다양한 산업체들의 양자키분배 시스템 개발에 활용 가능하며, 상호 운용성 확보에도 기여 가능</td></tr>
<tr><td>전략적 중요도 / 국내 역량</td><td colspan="2"> 
</td><td>표준화 기구/ 단체</td><td>국내</td><td>TTA 광전송 PG, 미래양자융합포럼</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td>국제</td><td>ETSI QKD/QSC, ITU-T SG13/ SG17, IETF</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td>국내 참여 업체/ 기관</td><td>SKT, KT, ETRI, KIST</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="4">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td></tr>
<tr><td>국외</td><td colspan="4">□기초연구↦□실험↦□시작품↦□제품화↦■사업화</td></tr>
<tr><td>선도국가/기업</td><td colspan="2">(미국) Battelle, (중국) Huawei/QuantumCtech, (일본) Toshiba</td><td>기술 수준</td><td>85% (선도국가대비)</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="4">□표준기획↦□의제연구↦□항목승인↦■표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>국제</td><td colspan="4">□표준기획↦□의제연구↦□항목승인↦■표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>선도국가/기업</td><td colspan="2">(일본) Toshiba, (캐나다) Waterloo University, (중국) Huawei</td><td>표준 수준</td><td>80% (선도국가대비)</td></tr>
<tr><td colspan="6">- Trace Tracking : 추격/협력공략(Ver.2023 신규)
ETSI, ITU-T에서 QKD 구성 요소 및 제어 기술, 인터페이스에 대한 표준화가 진행되었음. 해당 표준들은 QKD 시스템 개발에 필수적인 기술이며, 지속적으로 보완될 것으로 예상됨. 국내에서는 해당표준들의 도입 중심으로 표준화가 진행되고 있으나, 국내 개발 기술의 표준 반영을 위해서는 다각적인 협력이 필요하므로 추격/협력공략 항목으로 분류함</td></tr>
</table>



< 국제표준화 대응체계 >

국제 표준화 추진 전략	**<표준화 계획>** - ETSI QKD ISG, ITU-T에서 QKD 시스템 관련 표준화가 진행되었거나 진행되고 있으며, 새로운 프로토콜 및 방식(무선 등)의 양자키분배 개발과, 안전성 관련 요구사항을 반영한 양자키분배 시스템 개발이 증가하고 있어, 국제표준화가 증가될 것으로 예상됨 **<대응방안>** - (공식표준화 대응전략: 국제표준화기구 활동(적극대응)) ETSI QKD ISG에서 정리되는 QKD 시스템 관련 산업 규격에 대한 검토하고 분석 내용을 국내 산업계와 공유하여 차후 진행 가능성 있는 QKD 시스템 표준의 기술 방향에 대응하도록 유도함 - (사실표준화 대응전략: 사실표준화기구 활동(적극대응)) QKD 시스템 표준이 국제기구에서 진행 시 국내 산업계가 보유한 QKD 시스템 기술이 반영되도록 대응
국내 표준화 추진 전략	**<표준화 계획>** - 양자암호통신 및 QKD 시스템 기술 표준 관련 미래양자융합포럼과 기업 중심의 산·학·연 컨소시엄에서 국제 표준화를 위해 실제 표준 개발 및 ETSI, ITU-T와 연계한 표준화를 진행할 예정 **<대응방안>** - (표준화위원회 PG활동) QKD 시스템과 관련된 ETSI QKD ISG의 준용표준(TTAE.ET-GS 003 등)을 검토하여 새롭게 국내 환경에 최적화된 QKD 시스템 표준 개발 여부 판단 - (국제표준 준용) QKD 시스템에 대한 국제 표준화가 진행되면 적극 참여하여 자체 개발 또는 국제 표준 준용 여부 판단
표준특허 전략	- **(표준 및 R&D 중후기 전략 : 특허풀 대응을 위한 지분확대 및 권리 유연성 확보 전략)** ETSI ISG 국내 준용 표준과 국내 산업계 기술과의 연동성 상세 분석을 통해 자체 기술 특허와 표준 개발 유도
중단기 전략 (3개년)	

<table>
<tr><th colspan="6">(선도경쟁공략 | 병행) 양자키분배 프로토콜 및 키관리 표준</th></tr>
<tr><td>주요 내용</td><td colspan="5">ㅇ 양자키분배를 위한 양자계층, 키관리 계층, 제어계층 및 키 전달을 위한 프로토콜 표준 및 키관리 표준 개발</td></tr>
<tr><td>필요성</td><td colspan="5">ㅇ 양자키분배 기술의 성숙도는 높은 수준이나, 실제 키를 분배하기 위해 양자키분배 네트워크 내에서 사용되는 프로토콜은 키를 애플리케이션에 전달하는 인터페이스에 적용하는 프로토콜만이 표준으로 존재함
- 양자키 분배를 위한 양자키분배 네트워크 내의 다양한 인터페이스에서 사용되는 프로토콜 표준화 필요
- 양자키 분배를 위한 양자계층 프로토콜 표준화 필요</td></tr>
<tr><td rowspan="3">전략적 중요도 / 국내 역량</td><td colspan="2" rowspan="3"> 
</td><td rowspan="3">표준화 기구/ 단체</td><td>국내</td><td>TTA 응용보안/평가인증 PG</td></tr>
<tr><td>국제</td><td>ETSI ISG QKD, ITU-T SG11/SG13/ SG17</td></tr>
<tr><td>국내 참여 업체/ 기관</td><td>SKT,KT,ETRI, IDQ Korea</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="3">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td></tr>
<tr><td>국외</td><td colspan="3">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td></tr>
<tr><td>선도국가/기업</td><td>(스위스) ID Quantique, (일본) Toshiba</td><td>기술 수준</td><td>90% (선도국가대비)</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="3">■표준기획↦□의제연구↦□항목승인↦□표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>국제</td><td colspan="3">□표준기획↦□의제연구↦□항목승인↦■표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>선도국가/기업</td><td>(스위스) ID Quantique, (일본) Toshiba, (중국) CAS Quantum Networks, QuantumCTek</td><td>표준 수준</td><td>90% (선도국가대비)</td></tr>
<tr><td colspan="6">- Trace Tracking : 선도경쟁공략(Ver.2023 신규)
양자키분배 프로토콜 및 키관리 기술은, ETSI, ITU-T 등에서 양자키분배 네트워크에 적용하기 위해 활발히 논의가 진행 중이고, 세부 요구사항 및 관련된 프로토콜과 키관리 기술에 대한 세부사항 표준화가 진행 중인 단계이므로 선도적 표준화 대응이 필요하여 Ver.2023에서 선도경쟁공략 항목으로 분류</td></tr>
</table>



< 국제표준화 대응체계 >

국제 표준화 추진 전략

<표준화 계획>

- ITU-T SG11에서 양자키분배 키관리를 위한 양자키분배 네트워크 내 인터페이스 프로코콜 표준화가 진행 중으로 2023년 내 표준으로 완성될 것으로 예상됨.
- ETSI ISG-QKD 그룹에서 이기종 양자키분배 네트워크간 키 분배 표준화가 진행 중이며, 2년 내 관련 표준이 완성될 것으로 예상됨
- ITU-T SG17에서 양자키분배 네트워크 양자계층 프로토콜 표준화를 추진하고자 하는 움직임이 있으며, 향후 관련 표준화가 진행될 가능성 있음

<대응방안>

- (공식표준화 대응전략 : 국제표준화기구 활동(적극대응)) ITU-T SG11/SG17 및 ETSI ISG-QKD 그룹에서 진행되고 있거나 진행될 예정인 표준에 대한 면밀한 검토가 필요하며, 국내 업계의 요구사항과 개발 사항을 반영할 필요 있음

* 2023년에는 ITU-T SG11의 인터페이스 프로코콜 표준, 2024년에는 ITU-T SG17의 양자계층 프로토콜 표준화, 2025년에는 ETSI ISG-QKD 키관리제어계층 프로토콜 표준화가 완성되 것으로 예상됨에 따라 이에 대한 면밀한 검토와 국내 업계 요구사항 반영이 필요함

국내 표준화 추진 전략

<표준화 계획>

- ITU-T 제정 표준의 국내 준용 전략으로 계획

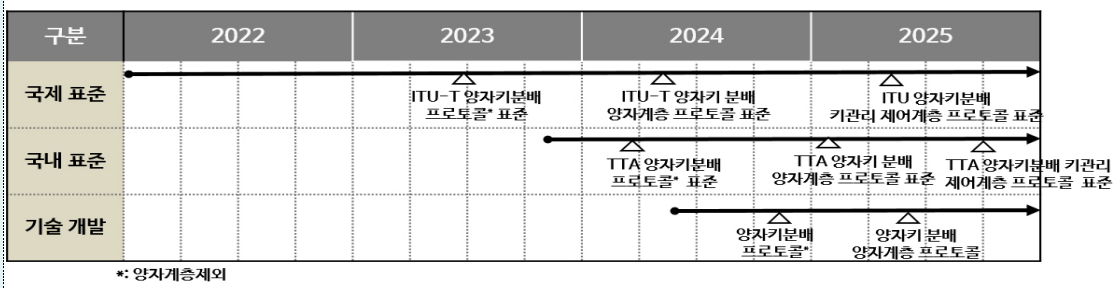
<대응방안>

- (국제표준 준용) ITU-T SG11/SG17 및 ETSI ISG-QKD 그룹에서 진행되거나 진행 예정인 국제 표준화 내용을 시차를 두고 국내표준으로 준용

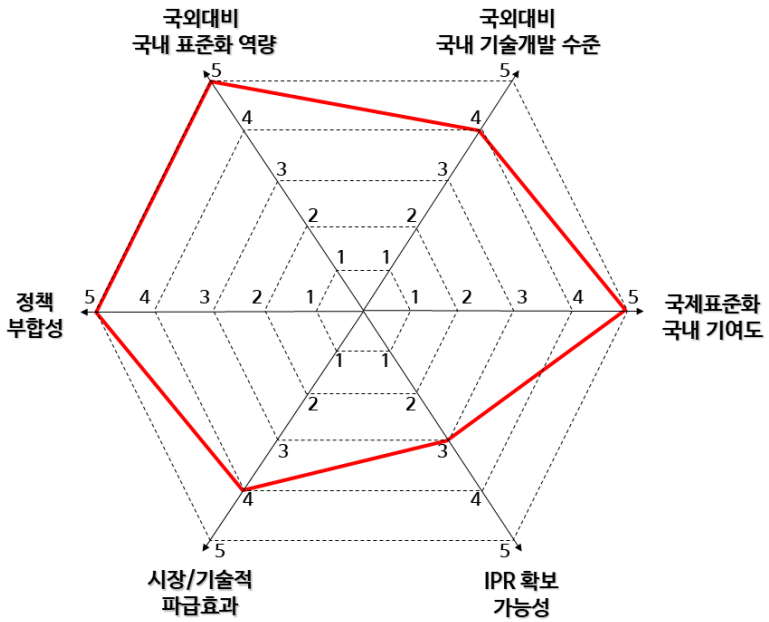
표준특허 전략

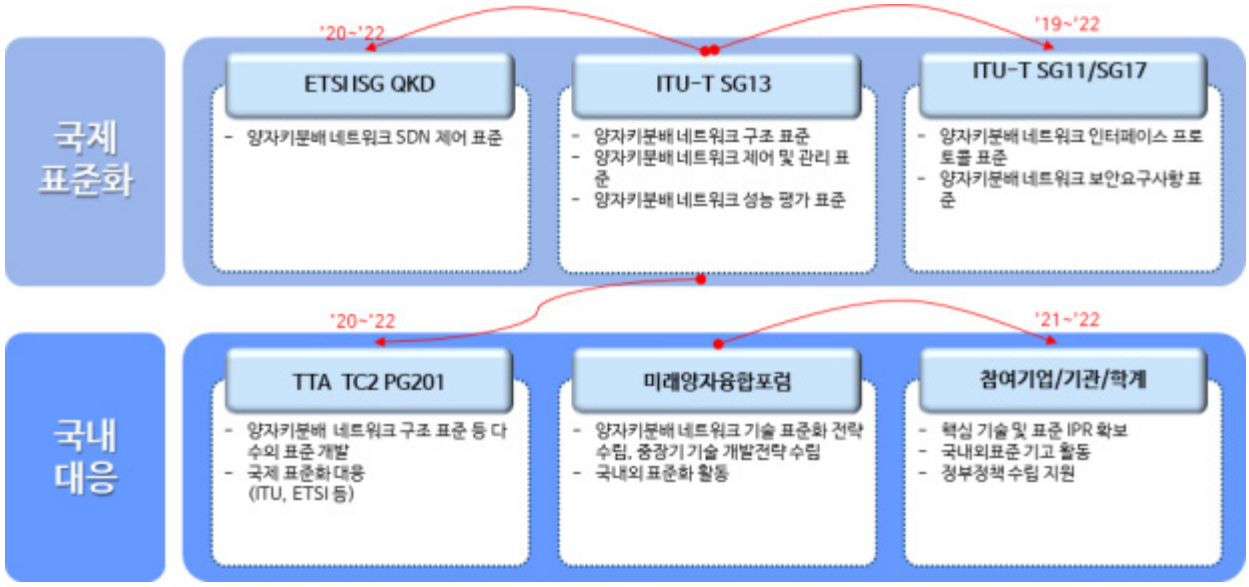
- **(표준 및 R&D 중후기 전략 : 특허 권리 범위 보완 전략)**양자키분배 프로토콜 및 양자계층 프로토콜에 대한 연구개발 및 개발 중 특허화 가능한 구현 특허 개발 및 권리 범위 확장 아이템 도출

중단기 전략 (3개년)



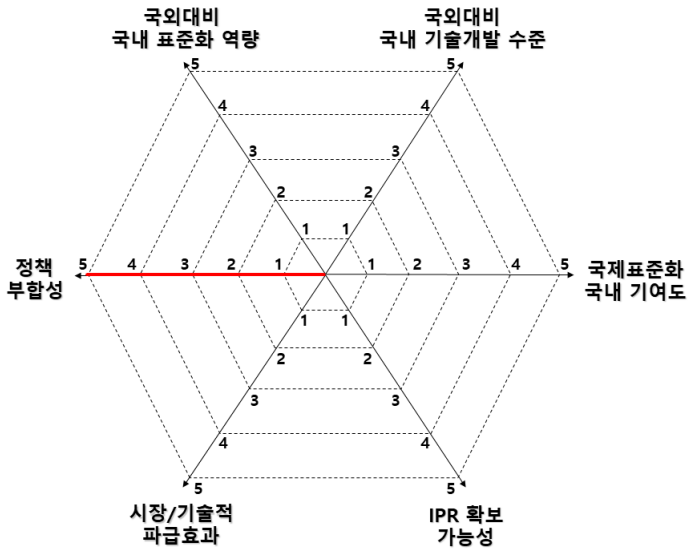
*: 양자계층제외

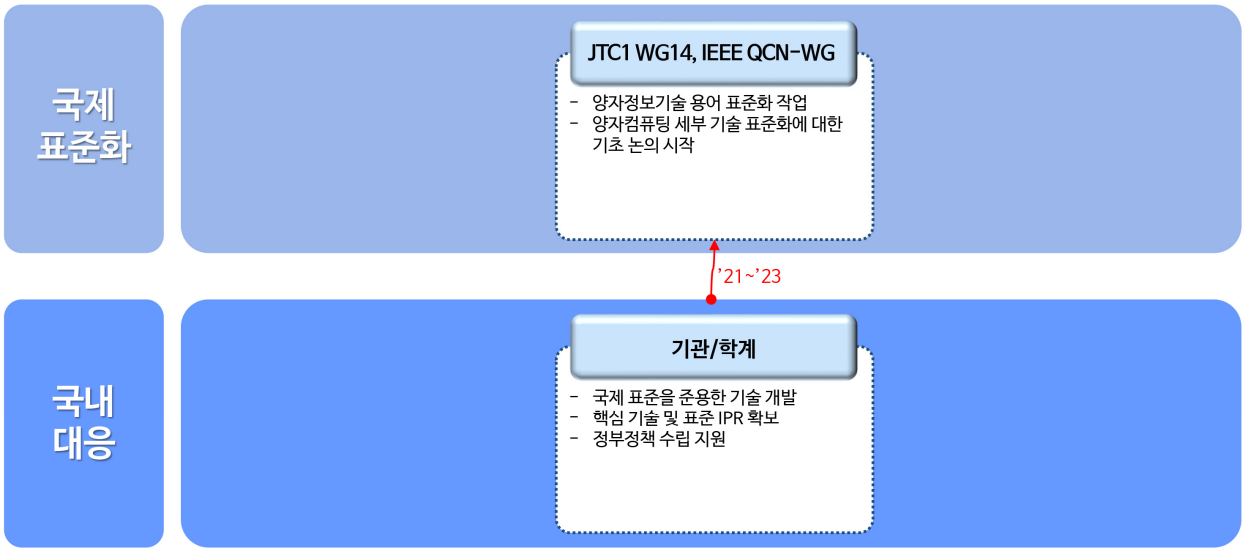
<table>
<tr><th colspan="6">(선도경쟁공략| 병행) 양자키분배 네트워크 및 망관리 표준</th></tr>
<tr><td>주요 내용</td><td colspan="5">ㅇ 양자키분배 기술의 네트워크화, 양자키분배 네트워크 제어 및 관리, 이기종 네트워크 연동 구조 및 인공지능 연계 구조 표준화 선점
- 양자키분배망 네트워크 구조 및 관리 기술 표준
- 양자키분배망 이기종 연동 인터페이스 및 구조 표준</td></tr>
<tr><td>필요성</td><td colspan="5">ㅇ 양자키분배 기술의 네트워크화 및 네트워크 관리 기술 표준은 다양하게 진행중이며, 각 국의 기술 표준화 선점 경쟁이 치열함
- 해당 기술의 표준화 경쟁 및 국내 기술의 국제 표준화를 위해 적극적 개발 필요
ㅇ 이기종 양자키분배망의 연동 및 제어 기술은 이제 표준화가 시작되는 단계로, 대규모 네트워크화를 위한 구현 목표 및 방향성을 결정하고 선점하기 위한 표준 및 관련 기술 개발 필요</td></tr>
<tr><td>전략적 중요도 / 국내 역량</td><td colspan="3"> 
</td><td>표준화 기구/ 단체</td><td>국내</td><td>TTA
광전송PG,
미래양자융합
포럼</td></tr>
<tr><td></td><td></td><td></td><td></td><td>국제</td><td>ITU-T SG11/
SG13/SG17,
ETSI ISG
QKD</td></tr>
<tr><td></td><td></td><td></td><td></td><td>국내 참여 업체/ 기관</td><td>KT, KAIST,
ETRI, SKT,</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="4">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td></tr>
<tr><td>국외</td><td colspan="4">□기초연구↦□실험↦□시작품↦■제품화↦□사업화</td></tr>
<tr><td>선도국가 /기업</td><td colspan="2">(유럽) Toshiba EU</td><td>기술 수준</td><td>90%
(선도국가대비)</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="4">■표준기획↦□의제연구↦□항목승인↦□표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>국제</td><td colspan="4">□표준기획↦□의제연구↦□항목승인↦■표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>선도국가 /기업</td><td colspan="2">(한국) KT, (중국) CAS Quantum Networks,
(유럽) Toshiba EU</td><td>표준 수준</td><td>100%
(선도국가대비)</td></tr>
<tr><td colspan="6">- Trace Tracking : 선도경쟁공략(Ver.2023 신규)
ITU에서는 양자암호통신 네트워크를 위한 국제표준 개발이 수십 건에 걸쳐 이뤄지고 있으며, 각국에서는 자국의 기술을 표준화 하기위해 치열한 경쟁을 펼치고 있음, 한국에서는 약 40%에 달하는 양자암호통신 네트워크 관련 표준 개발을 주도하고 있음을 감안하여, '선도경쟁공략'으로 명시하였음</td></tr>
</table>



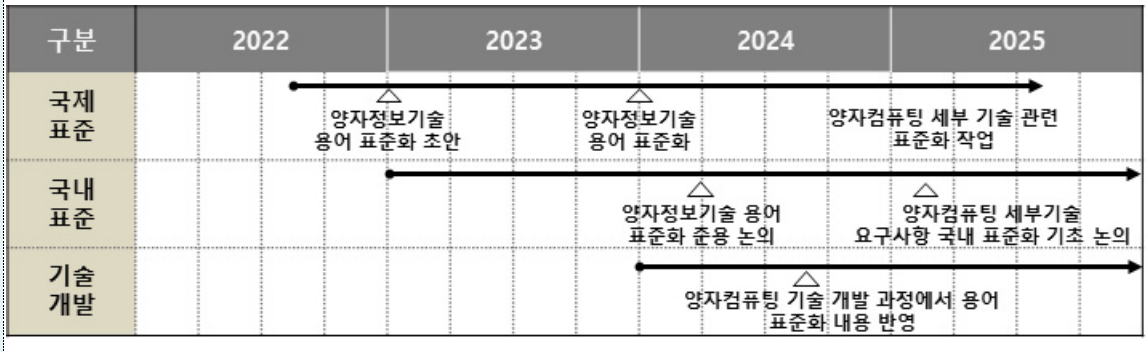
< 국제표준화 대응체계 >

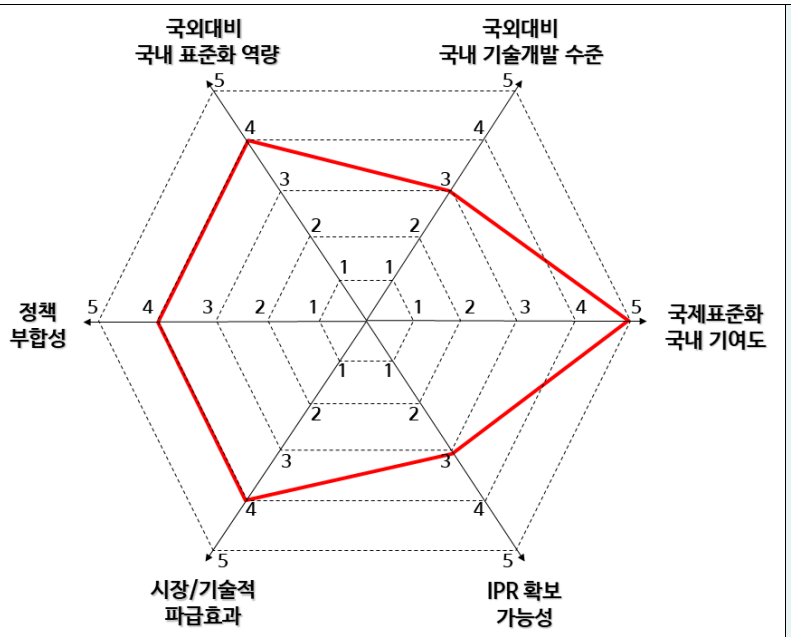
국제 표준화 추진 전략	**<표준화 계획>** - 양자암호통신 네트워크의 대규모 확장을 위한 양자암호통신 네트워크 제공 사업자간 연동과 관련된 표준, 양자암호통신 네트워크망 성능평가 표준, 기계학습 적용 네트워크 구축 및 제어/관리 표준 등을 개발하고 국제 표준화 선점 **<대응방안>** - (공식표준화 대응전략 : 국제표준화기구 활동(적극대응)) 한국이 주도권을 가지고 있는 ITU-T SG13을 필두로 한 지속적인 표준 개발을 통해 양자암호통신 네트워크 구조 관련 시리즈 표준들의 표준화 및 글로벌 리더십 지속 추진
국내 표준화 추진 전략	**<표준화 계획>** - 한국 주도로 개발중인 국제 표준과 연계하여 양자암호통신 네트워크 구조, 사업자간 연동 기술, 네트워크 망 성능 평가 표준등의 국내 표준화 추진 **<대응방안>** - (표준화위원회 PG활동) 광전송 프로젝트 그룹을 통해 양자암호통신 네트워크 관련 다양한 표준을 국내/국제표준 동시 개발
표준특허 전략	- **(표준 및 R&D 중후기 전략 : 표준 정합성 확보를 위한 특허 재설계 전략)** ITU-T에서 개발중인 국제표준과 국내 산업계 관련 기술 및 특허 분석을 통해 기술특허 및 표준특허 확보를 위한 전략을 수립하고, 한국 주도로 개발중인 표준에 관련 특허 기술을 포함하는 전략 실행
중단기 전략 (3개년)	

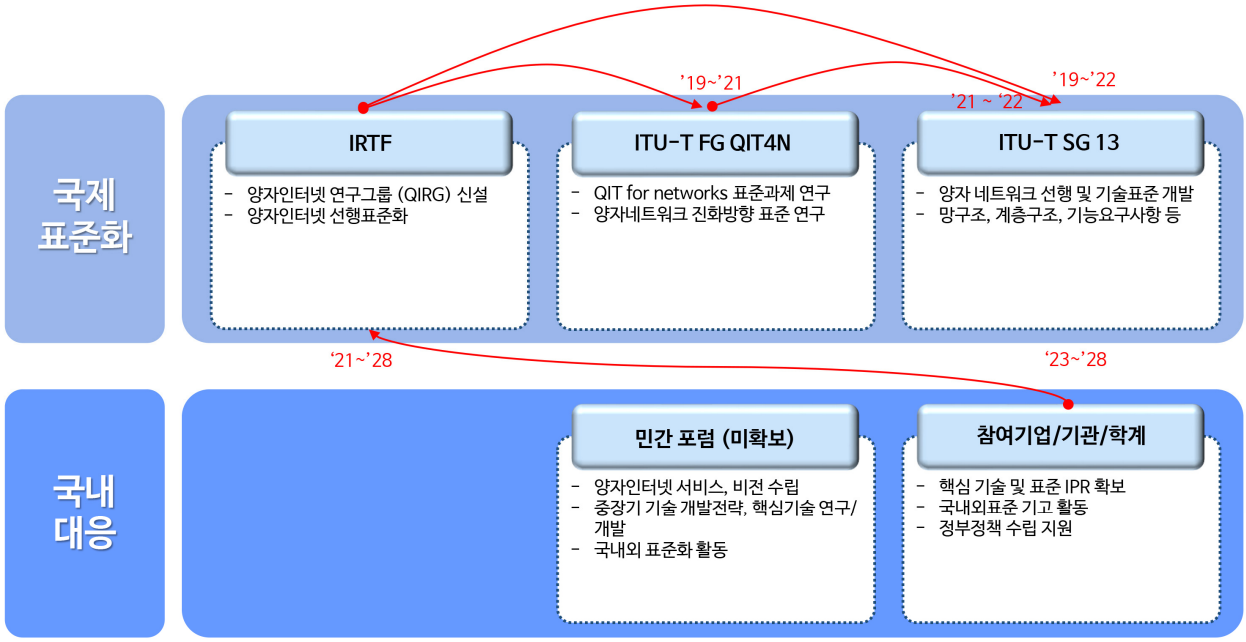
<table>
<tr><th colspan="6">(추격/협력공략 | 선행) 양자 컴퓨팅 용어 표준</th></tr>
<tr><td>주요 내용</td><td colspan="5">ㅇ 양자 기술에 대한 일반적인 명명법을 제공하여 양자기술의 하드웨어 및 소프트웨어 용어를 표준화하는데 활용
- 양자 터널링, 양자중첩, 양자 얽힘 같은 양자역학 관련 용어 외에도 초전도 양자 컴퓨팅, 이온트랩, 광격자, 핵자기 공명 같은 양자정보기술 하드웨어 관련 용어를 포함</td></tr>
<tr><td>필요성</td><td colspan="5">ㅇ 신산업에 속하는 양자정보기술의 연구개발 초기 과정에서 서로 파편화되고 상이하게 사용되는 용어들을 표준화할 필요가 있음
- 양자정보기술 소프트웨어 및 하드웨어 개발자 그룹과 양자 기술의 사용자 (엔지니어, 수학자, 물리학자, 화학자, 기후과학자, 생물학자 등) 그룹이 양자 정보 기술에 더욱 쉽게 접근할 수 있게 함</td></tr>
<tr><td>전략적 중요도 / 국내 역량</td><td colspan="3"> 
</td><td>표준화 기구/ 단체</td><td>국내</td><td>-</td></tr>
<tr><td></td><td></td><td></td><td></td><td>국제</td><td>JTC1 WG14, IEEE QCN-WG</td></tr>
<tr><td></td><td></td><td></td><td></td><td>국내 참여 업체/ 기관</td><td>-</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="4">■기초연구↦□실험↦□시작품↦□제품화↦□사업화</td></tr>
<tr><td>국외</td><td colspan="4">□기초연구↦■실험↦□시작품↦□제품화↦□사업화</td></tr>
<tr><td>선도국가 /기업</td><td colspan="2">(미국) IBM, Google</td><td>기술 수준</td><td>50% (선도국가대비)</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="4">■표준기획↦□의제연구↦□항목승인↦□표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>국제</td><td colspan="4">□표준기획↦□의제연구↦□항목승인↦■표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>선도국가 /기업</td><td colspan="2">(미국) IBM, Google</td><td>표준 수준</td><td>50% (선도국가대비)</td></tr>
<tr><td colspan="6">- Trace Tracking : 추격/협력공략 (Ver.2023 신규)
- 미국 IEEE의 QCN-WG에서 양자정보통신 기술개발에 사용되는 양자역학 용어와 양자정보통신 기술의 기술적 용어를 표준화하기 위한 작업이 진행중임. 반면, 국내의 경우 관련 항목을 포함하여 양자컴퓨팅 기술에 대한 표준화가 진행되지 않고 있음. 이에, “추격/협력공략” 으로 명시하였음</td></tr>
</table>



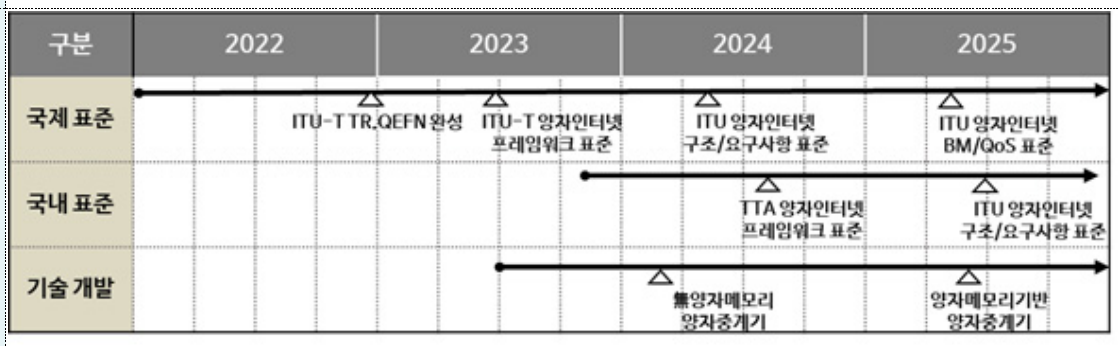
< 국제표준화 대응체계 >

국제 표준화 추진 전략	**<표준화 계획>** - 양자역학 및 양자정보 기술의 용어에 대한 표준 정립('22년 말 초안작성) **<대응방안>** - (공식표준화 대응전략 : 사실표준화기구 활동(기초대응)) 현재 관련 표준화 작업이 진행되고 있는 사실 표준화기구(IEEE)에 활동함
국내 표준화 추진 전략	**<표준화 계획>** - 양자정보기술의 용어와 관련해서는 차별적인 표준을 새로 수립하는 대신 국제적으로 정립된 표준을 준용함 **<대응방안>** - (국제표준 준용) 국제표준 준용과 국내 양자컴퓨팅 기술 개발 진행을 통한 국내 표준 제정 필요
표준특허 전략	- **(표준 중후기 및 R&D 초중기 전략 : 표준안 공백분야 도출전략)** 양자컴퓨팅 및 양자기술 용어 표준내용을 기반으로 양자컴퓨팅 기술 개발을 수행하고, 이 과정에서 중요 결과물을 특허로 출원하고 동시에 표준화 활동을 통해 표준에 반영 - 양자컴퓨팅 기술별 표준 요구사항을 분석하고, 그 결과를 토대로 기 보유한 특허 중 표준안에 부합하는 특허를 수정 보완하여 표준특허로 발굴함
중단기 전략 (3개년)	

<table>
<tr><th colspan="6">(차세대공략 | 병행) 양자 네트워크 구조 표준</th></tr>
<tr><td>주요 내용</td><td colspan="5">○ 양자암호통신 표준화 성과를 기반으로, 양자 컴퓨팅·양자 센싱 기술의 네트워크화 표준 개발과 양자인터넷 프레임워크 표준화 선점
- 양자인터넷 선행표준(구조, 기술 요구사항, 인터페이스 규격 등)
- 글로벌 표준화 리더십 확보로 한국向 표준기술개발 유도 및 핵심표준 선점</td></tr>
<tr><td>필요성</td><td colspan="5">○ 초기 원천기술 개발 및 시험망 구축 단계인 양자 인터넷은, 양자기기 간 네트워크화 및 양자 중계기, 양자 라우터/스위치, 양자 인터페이스 등 핵심기술개발을 위한 방향성 및 구현 목표 확보 위한 표준기술 개발 필요
- (선행표준 선점) 양자인터넷 기본 아키텍처, 양자 네트워크 및 양자/Legacy 응용 서비스를 고려한 계층구조, 각 계층별 기능 요구사항(Functional Requirements), 상세 기술표준 개발을 위한 기술 요구사항(Technical Requirements) 표준 등을 개발하고 국제표준화 선점
- (기술표준 개발) 선행표준이 정의한 구조 및 요구사항 구현을 위한 구조 계층 내/계층 간 인터페이스 및 프로토콜, 양자네트워크 전송 및 스위칭, 양자인터넷 라우팅, 네트워크 성능, 서비스 품질, 사업자간/국가간 연동 표준 등을 개발하고 국내외 표준화 필요</td></tr>
<tr><td>전략적 중요도 / 국내 역량</td><td colspan="2"> 
</td><td>표준화 기구/ 단체</td><td>국내</td><td>-</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td>국제</td><td>ITU-T SG13, IRTF</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td>국내 참여 업체/ 기관</td><td>KT, KAIST, ETRI</td></tr>
<tr><td rowspan="3">기술 개발 단계</td><td>국내</td><td colspan="4">■기초연구↦□실험↦□시작품↦□제품화↦□사업화</td></tr>
<tr><td>국외</td><td colspan="4">□기초연구↦■실험↦□시작품↦□제품화↦□사업화</td></tr>
<tr><td>선도국가 /기업</td><td colspan="2">(네덜란드) Delft, (EU) QIA, (미국) 아르곤연구소</td><td>기술 수준</td><td>80% (선도국가대비)</td></tr>
<tr><td rowspan="3">표준화 단계</td><td>국내</td><td colspan="4">■표준기획↦□의제연구↦□항목승인↦□표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>국제</td><td colspan="4">□표준기획↦■의제연구↦□항목승인↦□표준초안↦□표준승인/발간↦□표준활용/확산</td></tr>
<tr><td>선도국가 /기업</td><td colspan="2">(미국) IRTF</td><td>표준 수준</td><td>90% (선도국가대비)</td></tr>
<tr><td colspan="6">- Trace Tracking : 차세대공략(Ver.2023 신규)
: 미국 IRTF QIRG 그룹에서 양자 인터넷 표준화를 위한 기본기술 이해용 문서 작성이 진행 중이며, ITU에서는 SG13에서 양자인터넷 표준화 과제 (TR-QEFN)이 진행 중으로, 아직 구체적인 표준화 방향 및 표준문서 개발에 착수하기 직전임을 감안하여 차세대공략을 명시하였음.</td></tr>
</table>



< 국제표준화 대응체계 >

국제 표준화 추진 전략	**<표준화 계획>** - 양자인터넷 기본 아키텍처, 양자 네트워크 및 양자/Legacy 응용서비스를 고려한 계층구조, 각 계층별 기능 요구사항(Functional Requirements), 상세 기술표준 개발을 위한 기술 요구사항(Technical Requirements) 표준 등을 개발하고 국제표준화 선점 **<대응방안>** - (공식표준화 대응전략: 국제표준화기구 활동(적극대응)) 한국이 이니셔티브를 선점한 ITU-T SG13을 중심으로, TR-QEFN을 조기에 완성하고 후속 표준화로 양자 네트워크 구조 혹은 프레임워크 표준화 주도
국내 표준화 추진 전략	**<표준화 계획>** - ITU에서의 한국 주도 선행표준의 조기 국내 부합화 추진(TTA 단체표준) **<대응방안>** - (표준화위원회 PG활동) 양자인터넷 기본 아키텍처, 양자 네트워크 및 양자/Legacy 응용서비스를 고려한 계층구조, 각 계층별 기능 요구사항(Functional Requirements), 상세 기술표준 개발을 위한 기술 요구사항(Technical Requirements) 표준에 대한 국내 표준화 활동 필요
표준특허 전략	- **(표준 및 R&D 초중기 전략: 표준화 방향에 따른 출원 및 기고 전략)** '양자네트워크 구조 표준'은 직접적인 특허 발굴의 기회는 제한적이나, 향후 본 선행표준 기반 기술표준화를 사전에 검토/발굴하여, 기출원된 국내 특허를 기술표준에 반영하는 전략 실행
중단기 전략 (3개년)	

[작성위원]

구 분	소속	성명	직위	국내외 표준화활동
총괄	IITP	오윤제	PM	▸ 과기정통부 반도체·양자 PM
Ver.2023 분과장	NSR (국가보안 기술연구소)	권대성	연구 위원	▸ JTC1 SC27 전문가, 국가표준(KS) 정보보호 기술심의회위원
학	세종대	김아정	교수	▸ IEEE 1914, ETSI QKD ISG 활동 ▸ TTA 광전송 PG(PG201) 위원, 이더넷 PG(PG218), 정보보호 기반 PG(PG501) 위원, 한국 ITU-T SG15 연구반 위원
산	KT	김형수	팀장	▸ ITU-T SG13 부의장 수임 ▸ ITU-T SG13 WP1 의장 수임 ▸ 한국 ITU연구위원회 SG13연구반 반장
산	KT	윤춘석	선임	▸ ITU-T SG17 Q15 부라포처, JTC1 SC27 WG3 위원 ▸ 한국 ITU-T SG2 연구반 간사, SG13 연구반 간사, SG17 연구반 위원, TTA 광전송 PG(PG201), 사이버보안 PG(PG503), 응용보안/평가인증 PG(PG504) 위원
산	SKT	심동희	팀장	▸ ITU-T SG17 Q15 라포처, ITU-T SG13 Q16 에디터, JTC1 SC27 WG3 위원 ▸ ETSI 018 표준 에디터 ▸ 한국 ITU-T SG17 연구반 위원
연	KRISS (한국표준 과학연구원)	박희수	책임	▸ TTA 표준화 전략맵 양자정보통신의 양자센서 분과 위원 ▸ BIPM(국제도량형국) 광자측정표준(CCPR) 그룹 참여
연	ETRI	황용수	기술 총괄	▸ TTA 표준화 전략맵 양자정보통신의 양자컴퓨팅 분과 위원
연	NSR (국가보안 기술연구소)	홍창호	선임	TTA 응용보안/평가인증 PG(PG504) 위원
연	KIST (한국과학 기술연구원)	한상욱	책임	▸ TTA 표준화 전략맵 양자정보통신의 양자컴퓨팅 분과 위원
특허분석	광앤장 특허법인	장홍석	변리사	▸ TTA 표준화전략맵 양자정보통신 분야 특허분석 담당
TTA PG 담당	TTA	박수정	책임	▸ TTA 표준화전략맵 양자정보통신 분야 PG 간사, TTA 정보보호기반 PG(PG501) 간사, 사이버보안 PG(PG503) 간사, 응용보안/평가인증 PG(PG504) 간사
TTA PG 담당	TTA	민선미	책임	▸ TTA 표준화전략맵 양자정보통신 분야 PG 간사, TTA 광전송 PG(PG201) 간사
사무국	TTA	전지윤	책임	▸ TTA 표준화전략맵 양자정보통신 분야 간사

[참고문헌]

1. 심동희, “ITU-T SG17 양자 암호 표준화 동향”, 정보보호학회지, 제29권 제4호
2. 심동희, “양자키 분배 네트워크를 위한 보안 요구 사항과 양자 난수 생성기 표준화 동향”, 정보보호학회지, 제30권, 제4호
3. 심동희, “양자 암호 보안 표준화 동향”, 정보보호학회지, 제31권, 제4호
4. 심동희, “양자 키 분배 기술을 활용한 하이브리드 키 교환 방법”, 제32권 제4호
5. TTAK.KO-12.0356, 양자키분배 보안 요구사항, 2019.12
6. TTAK.KO-12.0329-Part1, 양자 키 분배 - 제1부: 일반, 2018.12
7. TTAK.KO-12.0329-Part2, 양자 키 분배 - 제2부: BB84 프로토콜, 2018.12
8. ITU-T Y.3807, ITU-T Recommendation Y.3807, “Quantum key distribution networks - Quality of service parameters”, 2022.02
9. ITU-T XSTR-HYB-QKD, ITU-T Technical Report XSTR-HYB-QKD, “Overview of hybrid approaches for key exchange with QKD”, 2022.05
10. ITU-T Y.3805, ITU-T Recommendation Y.3805, “Quantum key distribution networks - Software-defined networking control”, 2021.12
11. ITU-T X.1712, ITU-T Recommendation X.1712, “Security requirements and measures for quantum key distribution networks - key management”, 2021.10
12. ITU-T X.1710, ITU-T Recommendation X.1710, “Security framework for quantum key distribution networks”, 2020.10
13. ITU-T X.1714, ITU-T Recommendation X.1714 “Key combination and confidential key supply for quantum key distribution networks”, 2020.10
14. ITU-T XSTR-SEC-QKD, ITU-T Technical Report XSTR-SEC-QKD,
15. ITU-T Y.3804, ITU-T Recommendation Y.3804, “Quantum key distribution networks - Control and management”, 2020.09
16. ITU-T Y.3801, ITU-T Recommendation Y.3801, “Functional requirements for quantum key distribution networks”, 2020.04
17. “Security considerations for quantum key distribution network”, 2020.03
18. ITU-T X.1702, ITU-T Recommendation X.1702, “Quantum noise random number generator architecture”, 2019.11
19. ITU-T Y.3800, ITU-T Recommendation Y.3800, “Overview on networks supporting quantum key distribution”, 2019.10

20. ETSI GS QKD 004, V2.1.1 “Quantum Key Distribution; Application Interface”, 2020.08
21. ETSI GS QKD 014, V1.1.1 “Quantum Key Distribution; Protocol and data format of REST-based key delivery API”, 2019.02
22. https://www.news1.kr/articles/?4531242
23. “Bright Nitrogen-Vacancy Centers in Diamond Inverted Nanocones,” Seong-Woo Jeon, Junghyun Lee, Hojoong Jung, Sang-Wook Han, Young-Wook Cho, Yong-Su Kim, Hyang-Tag Lim, Yanghee Kim, Matthias Niethammer, Weon Cheol Lim, Jonghan Song, Shinobu Onoda, Takeshi Ohshima, Rolf Reuter, Andrej Denisenko, Joerg Wrachtrup, and Sang-yun Lee, ACS Photonics 7, 2739 (2020)
24. “Error-mitigated photonic variational quantum eigensolver using a single-photon ququart,” Donghwa Lee, Jinil Lee, Seongjin Hong, Hyang-Tag Lim, Young-Wook Cho, Sang-Wook Han, Hyundong Shin, Junaid ur Rehman, and Yong-Su Kim, Optica 9, 88 (2022)
25. “Multiplexed sensing of magnetic field and temperature in real time using a nitrogen-vacancy ensemble in diamond,” Phys. Rev. Applied 17, 014009 (2022).
26. “Moving-frame imaging of transiting cold atoms for precise long-range transport,” M. Seo, I. H. Do, H. Lee, D.-H. Yu, S. Seo, H.-G. Hong, J. H. Han, S. E. Park, S.-B. Lee, T. Y. Kwon, J. Mun, and J. H. Lee, Opt. Express 30, 25707 (2022).
27. “Optimal teleportation via noisy quantum channels without additional qubit resources,” Dong-Gil Im, Chung-Hyun Lee, Yosep Kim, Hyunchul Nha, M. S. Kim, Seung-Woo Lee & Yoon-Ho Kim, npj Quantum Information, volume 7, Article number: 86 (2021년)
28. “Quantum Teleportation of Shared Quantum Secret,” Sang Min Lee, Seung-Woo Lee, Hyunseok Jeong, and Hee Su Park, Phys. Rev. Lett. 124, 060501
29. “Equitable multiparty quantum communication without a trusted third party,” Tanumoy Pramanik, Donghwa Lee, Young-Wook Cho, Hyang-Tag Lim, Sang-Wook Han, Hojoong Jung, Sung Moon, Kwang Jo Lee, and Yong-Su Kim, Phys. Rev. Applied 14, 064074 (2020)
30. “Fundamental building block for all-optical scalable quantum networks,”

Seung-Woo Lee, Timothy C. Ralph, and Hyunseok Jeong, Phys. Rev. A 100, 052303
31. W. Song et al., Quantum solvability of noisy linear problems by divide-and-conquer strategy, Quantum Sci. Technol. 7, 025009
32. H. Kim et al., Detailed balance of thermalization dynamics in Rydberg atom quantum simulators, Phys. Rev. Lett. 120, 180502
33. Frank Arute et al., Quantum supremacy using a programmable superconducting processor, nature 574, 550
34. Han-Sen Zhong et al. Quantum computational advantage using photons, science Vol. 370, Issue 6523, pp.1460-1463
35. Yulin Wu et al., Strong quantum computational advantage using a superconducting quantum processor, Phys. Rev. Lett. 127, 180501
36. Lars S. Madsen et al., Quantum computational advantage with a programmable photonic processor, nature 606, pp.75-81
37. Google Quantum AI, Exponential suppression of bit or phase errors with cyclic error correction, nature 595, pp.383-387
38. Google Quantum AI, Suppressing quantum errors by scaling a surface code logical qubit, arXiv:2207.06431
39. C. Ryan-Anderson et al., Realization of Real-Time Fault-Tolerant Quantum Error Correction, Phys. Rev. X 11, 041058
40. https://investors.rigetti.com/node/7401/pdf
41. https://ionq.com/posts/december-09-2020-scaling-quantum-computer-road map
42. https://www.quantinuum.com/pressrelease/quantinuum-announces-quant um- volume-4096-achievement
43. “Deterministic secure quantum communication on the BB84 system,” Y.-C. Jeong, S.-W. Ji, C. Hong, H. S. Park, and J. Jang, Entropy 22, 1268 (2020).
44. “Experimental realization of a four-photon seven-qubit graph state for one-way quantum computation,” S. M. Lee, H. S. Park, J. Cho, Y. Kang, J. Y. Lee, H. Kim, D.-H. Lee, and S.-K. Choi, Opt. Express 20, 6915 (2012).
45. https://biz.chosun.com/it-science/bio-science/2022/06/27/NOTIHMI4EZ D3XHDN5Z4HGVBCBQ/

46. https://www.yna.co.kr/view/AKR20211110086000063
47. ISO/IEC 23837-1, Information technology security techniques - Security requirements, test and evaluation methods for quantum key distribution - Part 1: Requirements
48. ISO/IEC 23837-2, Information technology security techniques - Security requirements, test and evaluation methods for quantum key distribution - Part 2: Evaluation and testing methods

[약어]

API	Application Programming Interface
CD	Committee Draft
CESI	China Electronics Standardization Institute
CNOT	Controlled-NOT
DARPA	Defence Advanced Research Projects Agency
DIS	Draft International Standard
ETSI	European Telecommunications Standards Institute
ETSI	European Telecommunications Standards Institute
FDIS	Final Draft International Standard
FTQC	Fault-Tolerant Quantum Computing (Computation)
HEMT	High Electron Mobility Transistor
IEC	International Electrotechnical Commission
IETF	International Engineering Task Force
IS	International Standard
ISO	International Organization for Standardization
ISO/IEC JTC1	ISO and IEC Joint Technical Committee (for information technology)
ITS	Information Theoretical Secure
KM	Key Management
KMS	Key Management System
NISQ	Noisy Intermediate-Scale Quantum
NMR	Nuclear Magnetic Resonance
NV	Nitrogen Vacancy
OTP	One Time Pad
QEC	Quantum Error Correction
QECC	Quantum Error-Correcting Code
QoS	Quality of Service
QRNG	Quantum Random Number Generator
QSDC	Quantum Secure Direct Communication
SG	Study Group
SQUID	Superconducting QUantum Interference Device
WD	Working Draft

1. 본 보고서는 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받은 과제(2022-0-00002, ICT 표준화 전략 및 기획 연구) 연구결과로 발간된 자료입니다.

□ 총 괄 책 임 자 : 구경철 (TTA 표준화본부장)
□ 사 업 책 임 자 : 김대중 (TTA 표준기획단장)
□ 표 준 기 획 단 : 오구영, 전보라, 고준호,
황유철, 전지윤, 조수진

ICT 표준화 전략맵 Ver.2023
양자정보통신

2022년도 12월 인쇄
2022년도 12월 발행

발 행 소 : 한국정보통신기술협회
발 행 인 : 최 영 해
발 간 번 호 : TTA-22114-SD
인 쇄 처 : (주)디자인여백플러스

한국정보통신기술협회
Telecommunications Technology Association
13591, 경기도 성남시 분당구 분당로 47
Tel : 010-5110-9946, Fax : 031-724-0109
http://www.tta.or.kr

ICT 표준화 전략맵

양자정보통신

ICT Standardization Strategy Map

TTA 한국정보통신기술협회
Telecommunications Technology Association

(13591) 경기도 성남시 분당구 분당로 47 Tel. 031-724-0114 www.tta.or.kr

94560

ISBN 979-11-89545-42-0