양자기술 현황과 전망

김영희 PG225(양자통신) 부의장, 한국지능정보사회진흥원 AI·양자기술활용팀 팀장

1. 머리말

2023년은 양자기술 도약의 원년이었다. 대한민국 정부는 2023년 6월 퀀텀코리아 2023에서 '대한민국 양자과학기술 전략'을 발표하였고, 국회에서는 2023년 10월 만장일치로 '양자과학기술 및 양자산업 육성에 관한 법률안(약칭: 양자기술산업법)'이 통과되어, 2024년 11월 법 시행을 앞두고 있다.

미국 정부도 2023년 11월 양자기술 산업화 역량 확보와 글로벌 리더십 유지를 위해 양자지원법 재승인(Reauthorized NQI Act)을 추진하여, 양자기술 실증 및 응용연구개발 지원, 테스트베드 조성, 산업화 촉진 및 인력양성 등으로 연구개발과 산업화를 연계하고 상호 협력하여 빠르게 양자산업 생태계를 조성하고 공급망을 확보하겠다는 강한 의지를 표명하였다.

양자기술산업법에 따라 한국지능정보사회진흥원(NIA)은 양자과학기술의 상용화 촉진(제14조), 양자산업 관련 기업의 창업 및 중소기업 육성(제16조) 등을 위한 전담기관 역할을 수행한다. 이는 양자정보통신기술의 진흥과 활성화 지원을 위해 2021년 6월 개정된 정보통신융합법(제27조의 2 제3항 및 같은 법시행령 제30조의 2)에 따라, 2022년 1월 '양자산업 활성화 및 생태계 지원' 전담기관으로 지정(과학기술정보통신부 공고 제2022-1033호)된 것을 계승한 것이다. 2024년 11월 양자기술산업법의 본격적인 시행에 맞춰, 한국지능정보사회진흥원은 양자기술의 산업화 활용 촉진을 위한 전담조직으로 'AI·양자기술활용팀'을 신설하고 종합적인 정책과 전문기술 지원체계를 준비하고 있다.

양자기술은 '중첩'과 '얽힘', '비가역성', '불확정성'이라는 초미시 세계의 양자 물리적 특성을 기존 정보통신 전 영역인 컴퓨팅, 통신, 센싱 분야에 적용하여 초고속 연산, 초신뢰 연결(보안), 초정밀 계측을 가능하게 한다. 이러한 양자기술 특성은 정보통신기술 영역뿐만 아니라 우주항공 및 해양, 인공지능, 바이오, 반도체 등 미래기술 영역은 물론 금융, 국방, 의료, 산업 등 미래 경제·사회 전반의 패러다임 변화와 혁신을 이끌 것으로 기대되어 미래 게임체인저 기술로 인식되고 있다. 또한 반도체 집적회로 성능이 2년마다 2배씩 증가한다는 무어의 법칙이 영원할 수 없으므로, 나노를 넘어 양자기술로의 변화는 불가피하다.

본고에서는 이러한 양자기술 중 가장 빠르게 상용화가 진행되고 있는 양자통신 분야의 양자암호통신기술을 중심으로 기반 기술 준비 현황과 향후 글로벌 표준경쟁에 대비하여 우리가 준비해야 할 사항을 논의해 보고자 한다.

< 양자역학 원리 > 양자는 더 이상 작게 나눌 수 없는 에너지 최소단위로 고전 물리학과 다른 ❶ 중첩성, ❷ 얽힘, ❸ 불확정성, ❹ 비가역성 특성을 가짐

중첩성	얽힘	불확정성	비가역성
0 1	0 1	?	? 1
'0'이면서 동시에 '1'인 상태	두 개의 양자 간 강한 특수관계	확률로 존재하는 임의의 상태	관측 후 복원 불가능

[그림 1] 양자암호통신 및 양자역학 원리

2. 양자암호통신 기술 개요

양자암호통신이란 양자역학 원리를 이용하여 도청 및 감청, 해킹이 원천적으로 불가능한 안전한 차세대 통신기술로, 송신자와 수신자 사이에 단일 광자 또는 공유된 얽힘 상태의 비국소성, 비가역성, 불확정성 원리를 활용하여 암호키 분배, 서명, 인증, 데이터 암호전송 등에 있어 도청이 불가능한 암호 기능을 구현하는 기술이다.

AI와 5G 등 ICT 발전에 따른 디지털 대전환은 산업구조의 디지털 기반 재편은 물론 경제, 사회, 문화 등 우리의 업무환경과 일상 생활 전반에서 디지털 의존도를 증가시킨다. 블록체인, 전자상거래 등에서 대부분의 보안 기능을 담당하는 공개키 암호방식 중 주로 사용되는 RSA[1]는 소인수분해 기반의 암호체계로, 수학적인 계산 복잡성에 기반하여 암호해독까지 오랜 시간이 걸린다는 점을 이용한 것이다.

고전 컴퓨터는 0 또는 1로 표시되는 2진법 비트를 활용하여 연산을 수행하는 반면, 양자컴퓨터는 큐비트(Q-bit)를 사용하여 0과 1이 중첩된 상태로 연산을 수행하므로 큐비트의 수(n)에 따라 기존 이진법 처리량의 n제곱 배만큼 빠른 속도로 연산을 처리할 수 있다. 이처럼 매우 짧은 시간에 초고속 연산이 가능한 양자컴퓨터의 등장은 현대 암호체계를 무력화시킬 수 있고, 이러한

1) RSA: Ron Rivest, Adi Shamir, Leonard Adleman 3명의 연구자 이름 앞 글자를 딴 것으로 공개키 암호화뿐만 아니라 전자서명이 가능한 최초의 알고리즘

보안 위협은 미래 경제·사회에 큰 파급력을 일으킬 것으로 예상되므로 고전 컴퓨터 기반의 현대 암호체계의 변화는 불가피해진다.

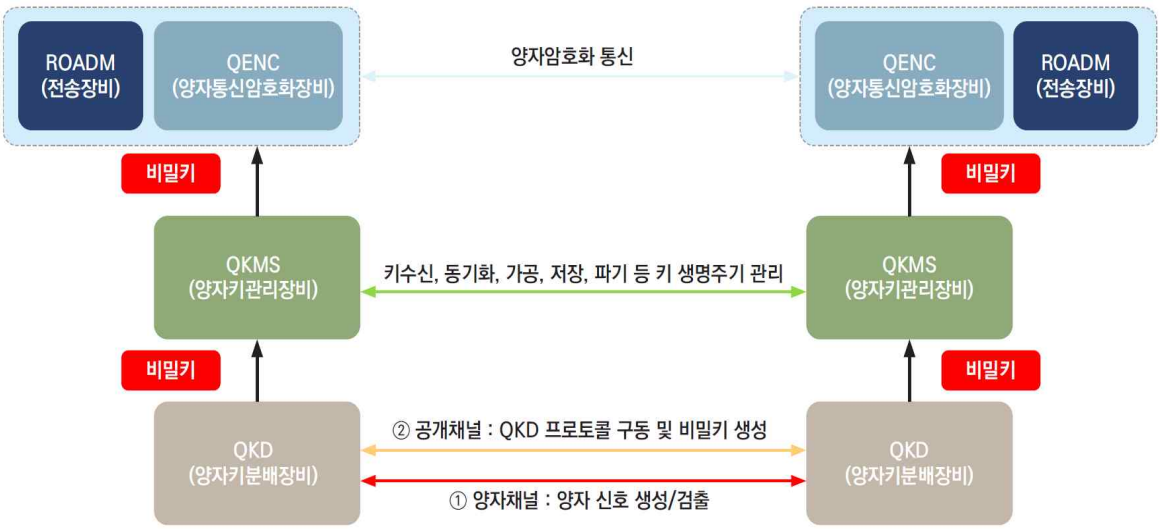
미래에 도래할 양자컴퓨터의 보편적 상용화에 대비하여, 기술적인 준비와 더불어 국가 암호체계의 재설계를 위한 중장기적인 정책적 준비와 현장 중심 실증이 필요하며, 국내외에서 양자의 물리적 특성을 이용한 QKD[2] 기반 양자암호통신, 수학적 알고리즘에 기반하는 PQC(양자내성암호)[3] 등의 연구개발 및 실증이 활발히 이루어지고 있다.

3. 양자암호통신 기술 실증

양자암호통신은 과학기술정보통신부와 한국지능정보사회진흥원이 2020년부터 추진한 '양자암호통신 인프라 구축 시범사업'을 통해 국내 공공과 민간분야에 빠르게 적용되어 시장 창출을 위한 초기 레퍼런스 확보 및 기술 국산화가 진행되었다.

시범사업 성과로, 2022년 7월 세계 세 번째로 통신 3사가 양자암호통신 기반 전용회선 서비스를 상용화하고 요금제도를 마련[4]하였고, 2023년 4월 과학기술 정보통신부와 국가정보원 및 NIA·NSR·ETRI·TTA 협력으로 세계 최초로 양자암호통신 장비에 대한 보안기능 검증제도(국가용 보안요구사항 152개 항목 확인)를 시행하였다. 따라서 공공과 민관 기관에서 양자암호통신 장비를 직접 도입하여 구축하거나 통신사로부터 양자암호통신 기반 전용회선서비스를 신청하여 이용할 수 있는 기술적·제도적 기반이 마련되었다.

양자암호통신은 [그림 2]과 같이 QKD, QKMS, QENC 3종의 장비로 구성된다. QKD 장비를 기반으로 양자역학 원리를 이용하여 신뢰하는 두 노드 사이에 단일광자(양자)로 비밀키를 생성하고 안전하게 분배하여 불법 도감청 및 도청이 불가능한 양자암호통신을 수행한다.



[그림 2] 양자암호통신 구성도

2) QKD: Quantum Key Distribution(양자 키 분배), 1984년 C. H. Bennett과 G. Brassard가 제안한 기술로, 양자의 물리적 특성을 이용하여 대칭 암호키를 생성하는 기술

3) PQC: 양자내성암호(Post-Quantum Cryptography), 양자컴퓨터의 공격에도 안전한 수학적 알고리즘에 기반한 암호체계로 격자 기반, 코드 기반, 다변수 기반, 해시 기반 암호 등으로 구분

4) 양자암호통신 기반 전용회선 서비스: SKB QKD기반 10G/100G 전용회선 상품 출시(2022.7), KT QKD기반 1G/10G 전용회선 상품 출시(2022.7), LGU+ PQC기반 10G 전용회선 서비스 출시(2022.4)

QKD(Quantum Key Distributor)는 양자키분배 장비로 양자채널을 이용하여 원격지의 QKD 간 안전한 양자암호키를 생성하고 분배하여 상호 공유한다. QKMS(Quantum Key Management System)는 양자키관리장비로 QKD로부터 비밀키를 전달받아 키의 동기화와 저장·파기 등 생명주기를 관리한다. QENC(Quantum Encryptor)는 양자통신암호화장비로 QKMS로부터 비밀키를 공급받아 종단간 데이터 전송을 위한 양자암호통신을 수행한다.

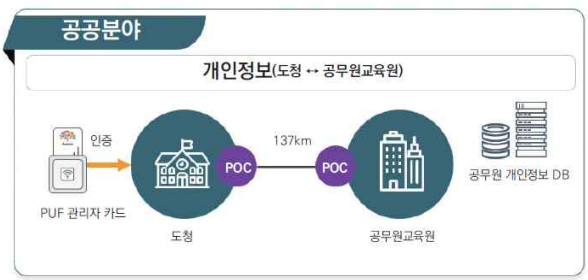
일반적으로 도청자는 정보를 탈취하기 위해 송신자와 수신자 간 전송되는 양자를 가로채고, 동일한 상태의 양자를 생성하여 수신자에게 전송하는 차단-재전송 공격(Intercept-resend attack)을 시도한다.

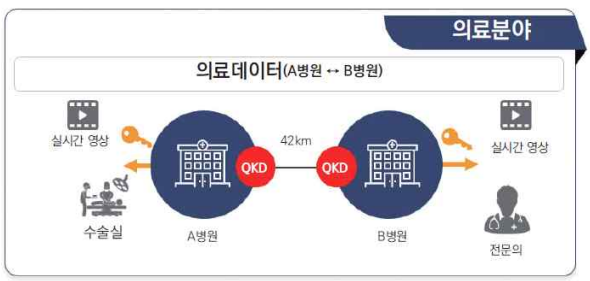
하지만 가로챈 양자의 상태를 측정하면 양자 상태가 붕괴하는 양자의 비가역성 특성에 따라 탈취 후 정확한 상태를 복원할 수 없다. 이러한 특성은 양자암호키 분배 프로토콜인 BB84 기반 송신자와 수신자간 큐비트 오류율(QBER) 측정 과정을 통해 양자암호통신의 초신뢰 보안을 제공하여 양자컴퓨터의 암호해독 위협에도 안전하다.

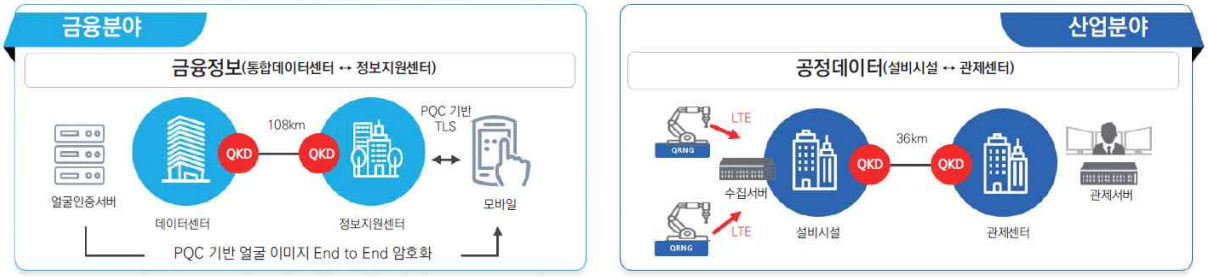
2022년까지 추진된 '양자암호통신 인프라 구축시범사업'으로 유선전송거리를 기존 80km에서 120km까지 확대하였고, 공공과 의료, 금융, 산업, 국방 분야 등 총 44개 양자암호통신 응용서비스 레퍼런스를 확보하고 국내 초기 시장을 창출하였다. 더불어 QKD 네트워크 구축 유형으로 기존 1:1 망구조에서 1:N 망구조, 신뢰노드 구조, 링(Ring) 구조 등으로 기술을 고도화하고 현장 실증을 추진하여 상용화를 위한 집선기술을 확보하였고, 수요기관 통신인프라 환경에 따른 다양한 양자암호통신 인프라 구성 및 비용 절감이 가능하였다.

<표 1> 양자암호통신 인프라 시범구축 기술고도화

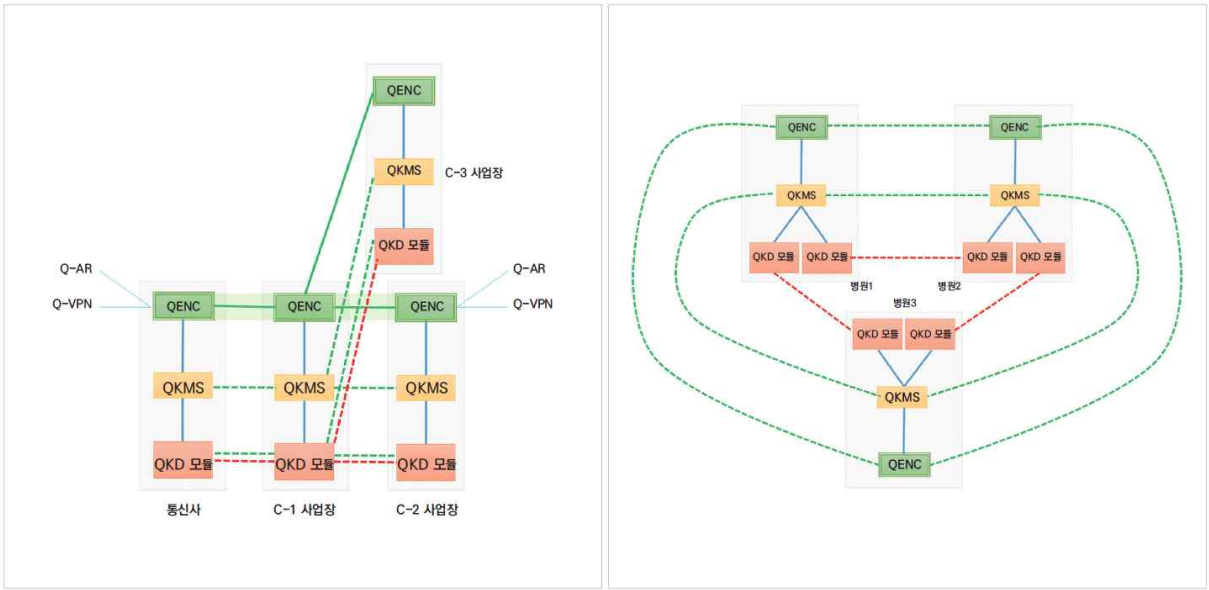
구분	2020년	2021년	2022년
유선거리	80km	100km	120km
양자키생성	10kbps	20kbps	30kbps
전송방식	유선	유선	유선/무선
망 관리	EMS	Q-SDN	이기종 제어 Q-SDN
광케이블	2개	2개	1개(WDM 적용)
응용서비스	기존 응용서비스 활용 (18개 구간)	QRNG기반 보안인증, 암호화 등 신규서비스(19개 구간)	AI, 양자센서 등 양자융합서비스(7개 구간)







[그림 3] 양자암호통신 시범구축 응용서비스 사례



※ 출처: TTA TTAK.KO-01.0235

[그림 4] 양자암호통신 시범구축 QKD 네트워크 사례

4. 양자암호통신 표준화

양자통신 분야에서 주도적 표준화 역할을 수행하기 위한 체계적 추진체계의 필요성에 따라, 2022년 12월 NIA·ETRI·KT·SKT·NSR 등이 참여하는 양자통신 프로젝트그룹(PG225)이 통신망 기술위원회(TC2) 산하에 신설되었다. 양자키 분배망의 공공기관 도입·운영 가이드가 TTA 고유 표준으로 2023년 12월 신규 제정되었다. 또 양자내성암호를 지원하는 전송망 프레임워크, 양자키 분배망 연동 시험 요구사항 등의 국내 표준화 활동을 하는 한편, ITU-T SG13, SG17, ETSI ISG QKD 등 국제표준화기구에서 제정된 국제표준안을 국내로 들여오는 준용 표준화 작업을 수행하고 있다.

TTA의 ICT표준화 로드맵 Ver.2024(양자정보통신)에 따르면, 양자암호통신과 양자네트워크 분야의 국내 역량과 기술성숙도를 고려하여 향후 표준화를 추진해야 하는 대상 기술은 <표 2>와 같다.

<표 2> 표준화 대상기술

표준화 대상 기술		세부 표준화 기술	비고
양자 암호 통신	QKD 프로토콜	• 키 분배를 목적으로 양자 기반 프로토콜 및 프레임워크 – 연속변수 및 분리변수 양자키 분배 규격, 준비 및 측정 – 측정장치, 양자얽힘 기반 양자키 분배 규격	표준R&D 추진필요
	양자 인증	• 무조건적 안전성을 지향하는 사용자/메시지 인증 기술 – 양자 얽힘 또는 단일광자 기반 양자 인증 프로토콜 – 양자인터넷 또는 양자네트워크 환경에서 양자 인증 등	R&D-표준 R&D 동시 추진필요
	QKD 후처리 기술	• QKD 후처리 프로토콜 및 규격 기술 – QKD 에러 정정, 비밀 증폭 등 후처리 관련 프로토콜 – QKD 후처리 규격 요구사항 또는 가이드라인	R&D-표준 R&D 동시 추진필요
	QKD 이기종 간 연동기술	• 이기종 QKD 장비 및 네트워크 연동 기술 – 양자키를 자동으로 암호화 장비에 제공하는 최적 경로 알고리즘 제어/운용 – 양자암호 장비와 제어 플랫폼 간 서비스 연동 및 품질 관리를 위한 제어/운용	R&D-표준 R&D 동시 추진필요
	QKD 부채널 위협 대응기술	• QKD 부채널 공격 대응 요구사항, 가이드라인 기술 – QKD 부채널 공격에 대한 대응 기술, – QKD 부채널 공격 대응 안전성 요구사항, 가이드라인	R&D 추진 필요
양자 네트 워크	양자 네트워크 프레임워크 참조모델	• 양자 네트워크 상세 기술규격 관련 표준화 이전 선행 참조모델 기술 – 양자 네트워크 계층 구조 참조모델 – 양자 네트워크 유스케이스 및 서비스 시나리오	R&D 추진 필요
	양자 네트워크 전송 계층 오류 정정	• 양자 네트워크 얽힘 정제 프로토콜 및 양자 상태 손실 보정 프로토콜 기술 – 얽힘쌍 생성 및 전송에서 발생하는 잡음감소 프로토콜 – 양자 네트워크를 통해 전달되는 양자 상태의 손실 및 오류 보정 프로토콜	R&D-표준 R&D 동시 추진필요

※ 출처: ICT표준화 로드맵 Ver.2024

현재까지 국산화 개발된 양자암호통신 장비와 기술들이 전국 기반 유무선 양자암호통신 인프라로 확대 구축되고 초신뢰 우주통신을 위한 위성 QKD, 양자네트워크 및 양자인터넷으로 발전되기 위해서는 표준을 기반으로 기술이 지속적으로 고도화되어야 한다. TTA PG225를 중심으로 QKD 프로토콜을 위한 표준화된 인증 및 프로세스, QKD 후처리 기술, 이기종 장비 간 상호운용성 및 품질 확보 등을 위한 국내 표준을 지속 개발하고 국제표준을 선점하기 위해 노력하여 미래 성장 동력을 꾸준히 확보해야 한다.

5. 맺음말

양자암호통신 기술이 국산 개발 상용화에 성공하였지만, 양자암호키 생성률 및 단일광자 최대 전송 거리 제약, 높은 양자암호통신 3종 장비 구매 가격, 양자채널을 위한 별도의 광케이블 필요 등으로 보편적 이용에는 아직 어려움이 있다. 향후 양자컴퓨터와 양자센서 등과 같은 양자기기를 상호 연결하여 양자 상태를 직접 전달하는 양자통신과 양자인터넷으로 발전하기 위해서는 양자암호통신 기술이 징검다리 역할을 해야 한다.

글로벌 시장조사 전문기관 Mind Commerce에 따르면, <표 3>과 같이 글로벌 양자통신 시장 규모는 2023년 말 5조 209억 원으로 추정되며 2026년에는 시장 매출액이 10조 원을 초과할 전망이다. 이 중 양자 키 분배(QKD) 시장은 연평균 19.9% 성장해 2029년 10조 원을 초과하여 2030년 12조 원 이상의 시장으로 성장할 것으로 전망된다.

<표 3> 글로벌 양자통신 시장 전망

(단위: 억원)

구분	2023	2024	2025	2026	2027	2028	2029	2030	성장률
양자통신	50,209	63,521	82,519	102,196	127,843	174,782	207,092	247,368	25.6%
QKD	34,196	43,424	54,009	61,744	73,278	93,633	108,967	121,773	19.9%

※ 출처: 2023 양자정보기술 백서

이에 양자암호통신 기술의 중요성을 인식하고, 기존 양자암호통신 기술 한계를 극복하고 산업확산을 촉진하기 위해서는 차세대 양자암호통신 기술로 지속 고도화하여 이미 확보된 글로벌 기술 경쟁력을 유지해야 한다. 따라서 양자암호통신의 저가격화에 필수적인 부품·장비 소형화와 집적화, 광 다 중화 기술기반 구축 비용 효율화, 표준 기반의 시스템 상호운용 및 품질 측정 기술, 양자 상태의 장거리 전송(500km 이상), 위성 양자 보안 통신을 위한 장거리 무선 QKD 기술 등의 연구개발이 정부의 연구개발 과제로 추진되고 있다.

또한 NIA는 2024년 신규 사업으로 전국 주요 거점(서울-KIST, 판교-NA/TTA, 대전-ETRI,KRISS 등)을 연결하는 양자기술 전용의 양자 테스트베드를 구축한다. 국내 중소기업과 산학연의 연구자들은 양자암호통신 산업화 기술, 양자통신과 양자센서 분야의 장비와 기술개발의 결과물을 전국 기반 상용망 수준의 테스트베드에서 시험·검증하고 양자기술 전문지원 서비스를 이용할 수 있다. 세계 최초로 국가정보원이 시행한 '양자암호통신장비 보안기능 검증 제도'의 안정적 안착을 위해서도 판교, 대전 거점에서 고가의 측정설비 활용, 인증 관련 사전 기술 컨설팅 등의 서비스를 제공받을 수 있다.

정부와 산학연의 긴밀한 협력을 바탕으로 각 기관들의 전문성과 역할이 균형적으로 발휘되고 극대화되어 양자의 '중첩'과 '얽힘'이라는 초미시 영역의 철학적 상상이 조기 현실화되고, 세계 최고 수준의 양자암호통신 국산화에 이은 성공모델이 양자센서 상용화, 양자 상태를 저장하는 양자메모리, 얽힘 기반의 양자인터넷 개발 등으로 연결되기를 기대한다.

[참고문헌]

[1] 김영희, 최진욱, 장유환, 국방 지능정보화 동향 제3호(양자암호통신 동향 및 국방적용 방향), 한국국방연구원, 2023. 02

[2] 한국지능정보사회진흥원, 양자기술 산업생태계 활성화 방안 발표 자료

[3] 한국정보통신기술협회, 정보통신단체표준(TTAS) TTAK.KO-01.0235, 양자키 분배방의 도입·운영 지침 및 활용 사례

[4] 국가정보원, '국가용 보안요구사항 V3.0' 양자암호제품군, 2023.03.

[5] 한국정보통신기술협회, ICT 표준화 로드맵 Ver.2024 (양자정보통신)

[6] 한국지능정보사회진흥원, 2023 양자정보기술백서

※ 출처: TTA 저널 제211호