양자보안 기술 및 국내외 동향

산업기술리서치센터 디지털·반도체팀
이수진 전임연구원(suzinlee@kdb.co.kr)

Ⅰ. 양자컴퓨터 및 현대 암호체계
Ⅱ. 양자보안 기술
Ⅲ. 국내외 동향
Ⅳ. 결론 및 시사

최근 주요국들은 양자기술을 국가 전략기술로 지정하고 기술개발에 박차를 가하고 있다. 특히, 양자컴퓨터는 고전컴퓨터보다 복잡한 계산과 데이터 처리를 훨씬 빠르게 해결하여 혁신적인 변화를 이끌 것으로 기대되고 있어 주요국과 글로벌 기업들이 앞다투어 개발에 뛰어드는 분야이다.

하지만 양자컴퓨터의 고속 연산능력은 역설적으로 현대 암호체계에 위협이 되고 있다. 특히 고전컴퓨터로는 풀 수 없는 암호화된 데이터를 미리 탈취·수집하여 향후 양자컴퓨터가 상용화 시 해독하는 HNDL(Harvest Now, Decrypt Later, 선취득 후해독) 공격은 이미 진행되고 있다.

이러한 보안 위협에 대응하여 양자보안 기술이 주목받고 있다. 대표적으로 기존 암호 알고리즘을 양자컴퓨터도 풀기 어려운 수준으로 업그레이드하는 양자내성암호(PQC, Post-Quantum Cryptography)와 양자역학을 이용해 해킹을 원천 차단하는 양자키분배(QKD, Quantum Key Distribution)가 핵심기술이다.

주요국들은 양자보안 기술 개발과 도입을 본격화하고 있다. 미국은 '31년까지 양자내성암호 전환 의무화를 추진 중이며, 중국은 세계 최대 양자키분배 실증 사업을 추진하고 있다. 우리나라도 양자내성암호 표준에서 강점을 보이는 등 충분한 기술 경쟁력을 보유하고 있다.

양자보안은 국가간 기술격차가 크지 않고 고성장이 예상되는 분야인 만큼, 초기 단계인 산업 특성상 서플라이체인 선점 시 주도권 확보도 가능하다. 특히, 우리나라는 세계 최고 수준의 통신망을 보유하고 있어 기술 상용화와 확산에 유리한 조건을 갖추고 있다. 양자보안 산업육성을 위해서는 요소기술 외에도 표준·인증 체계 정착을 위한 노력과 정부의 초기 수요 창출 등의 지원책이 필요하다.

* 본고의 내용은 집필자 견해로 당행의 공식입장이 아님

Ⅰ. 양자컴퓨터 및 현대 암호체계

❑ 양자컴퓨터는 고전컴퓨터에 양자역학을 접목한 것으로, 특정 연산에서 압도적 우위

○ 양자컴퓨터는 양자역학의 중첩[1]과 얽힘[2] 특성을 가지는 큐비트를 기본 단위로 하여 비트를 기본 단위로 하는 고전컴퓨터 대비 고속 연산이 가능

- 고전컴퓨터의 3비트는 (000)…(111) 총 8개 경우를 한번에 1개 정보만 처리, 양자컴퓨터의 3큐비트는 8개 경우가 동시에 존재해 한번에 모든 정보를 처리

〈표 1〉 고전컴퓨터와 양자컴퓨터

구분	고전컴퓨터(일반컴퓨터, 슈퍼컴퓨터)	양자컴퓨터
작동 원리	트랜지스터로 전기신호를 제어	양자역학을 정보처리에 적용
기본 단위	비트(Bit)	큐비트(Qubit, quantum bit)
예시	전기가 통하면 1, 안통하면 0	중첩으로 0과1을 동시에 구현
연산 방법	논리 표에 의한 반복 계산(직렬)	행렬 함수에 의한 동시 계산(병렬)
개념도	1개씩 순차적 계산 ⇩ 많은 시간 소요	합쳐서 한번에 계산 ⇩ 순식간에 계산

자료 : ETRI 등 산업 자료 종합, 당행 재구성

○ 시뮬레이션, 머신러닝과 같이 특정한 연산 환경에서, 양자컴퓨터의 연산 속도가 고전컴퓨터의 성능을 압도적으로 뛰어 넘는 '양자우위'를 달성

- 구글은 '19년 당시 최고 슈퍼컴퓨터로 1만년이 소요되는 연산을 자사의 양자컴퓨터(Sycamore)로 200초만에 해결했다고 발표하며 양자우위를 입증

○ 다만, 양자컴퓨터는 정답을 얻기 위해 반복 측정이 필요해 일상 작업에서는 고전컴퓨터 대비 비효율적으로 고전컴퓨터의 완전한 대체는 어려움

- 양자컴퓨터는 중첩 상태인 양자회로[3]의 연산 결과 측정(중첩 상태가 붕괴되고 하나의 값만 도출)을 반복하여 확률상 수렴되는 값을 정답으로 채택

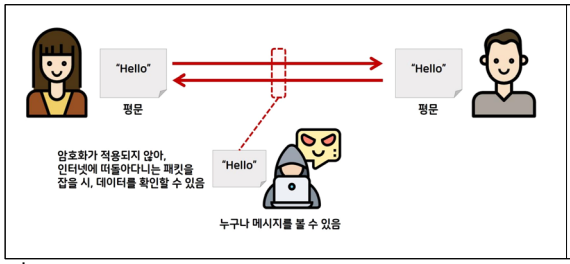
1) 중첩 : 모든 가능한 상태가 동시에 존재하는 현상, 큐비트는 0과1을 동시에 가져 병렬 연산 가능
2) 얽힘 : 한 양자의 상태가 확정되면 얽힘 상태의 연결된 양자의 상태도 즉시 결정되는 현상, 한 번의 조작으로 다수의 큐비트 상태를 동시에 처리할 수 있어 연산능력이 증가
3) 양자회로 : 고전컴퓨터의 논리회로처럼, 큐비트를 조작하여 연산을 수행하는 양자 계산의 설계도

❑ 현재 통신과정에서 정보는 대칭키와 공개키 방식의 암호화로 해커로부터 보호

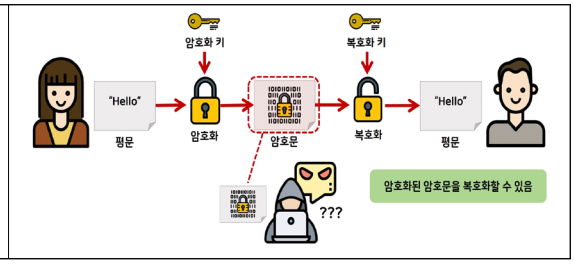
○ 통신과정에서 정보는 암호키를 이용한 암호화와 복호화(암호문을 평문으로 복원)로 해커의 접근을 제한

- 정보를 주고받는 통신채널은 주로 공개된 공간으로 정보의 탈취가 용이하기 때문에 평문을 해커가 중간에 탈취해도 해석하기 어렵도록 송신자는 암호키로 암호화하여 수신자에게 전송
- 암호키는 암호화와 복호화에 사용되는 비밀정보로, 암호키가 없으면 암호문을 해독할 수 없어 통신의 안전성은 암호키에 의존

〈그림 1〉 암호화 미적용시 정보 탈취



〈그림 2〉 암호화와 복호화

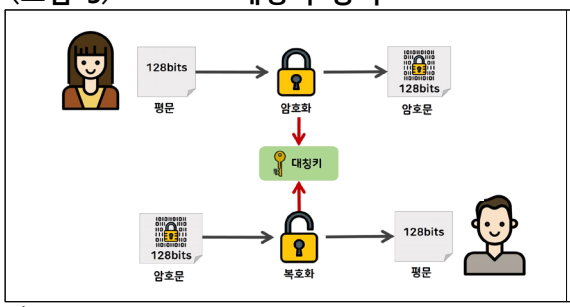


자료 : RAON CTF

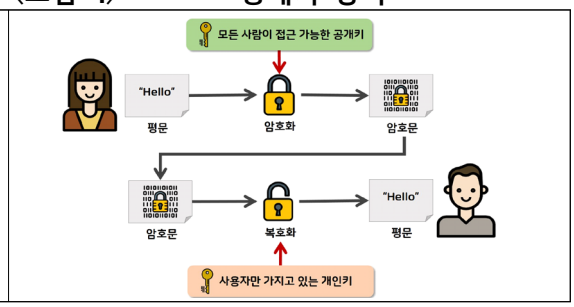
○ 현대 암호체계의 암호화 방식은 암호키의 특성에 따라 대칭키와 공개키로 구분

- 대칭키는 암호화와 복호화에 사전 분배한 하나의 동일한 비밀키를 사용
- 공개키는 암호화에 수신자가 모두에게 공개한 공개키를 사용하고 복호화에 수신자만 보관하는 개인키를 사용하여, 대칭키보다 보안을 강화
  · 일반적으로 사용하는 인터넷 보안의 90% 이상이 공개키 암호에 의존

〈그림 3〉 대칭키 방식



〈그림 4〉 공개키 방식



자료 : RAON CTF

Ⅱ. 양자보안 기술

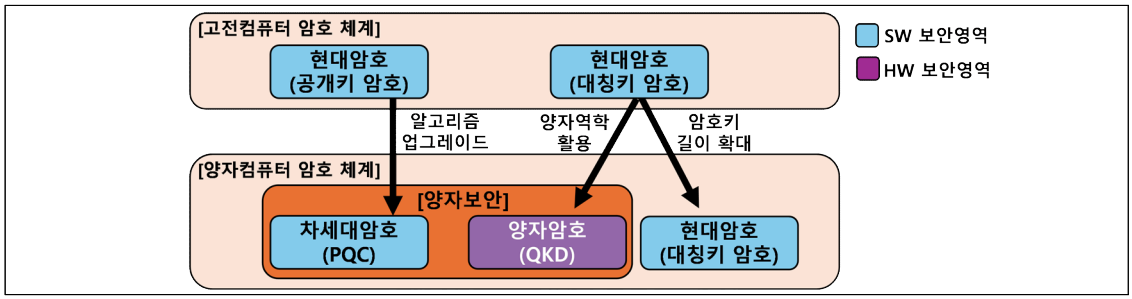
1. 양자보안 개요

❑ 양자보안은 양자컴퓨터 시대에 대응하는 암호 보안 체계로, 양자내성암호와 양자키분배 기술이 대표적

❍ 양자컴퓨터는 혁신의 핵심 동력이자 동시에 현대 암호체계의 근간을 흔들 수 있는 잠재적 위험 요인으로 평가
- 1천bit 숫자로 이루어진 암호를 소인수 분해하는데 고전 컴퓨터는 백만년이 소요되나, 양자컴퓨터는 1초~1일만에 해결 가능
- 양자컴퓨터의 고속 연산능력과 빠른 연산속도는 현대 암호체계를 위협하고, 이에 대응해 안전한 암호체계로 대비 및 전환하는 양자보안 기술이 대두

❍ 양자보안은 소프트웨어 기반의 양자내성암호(PQC, Post-Quantum Cryptography)와 하드웨어 기반의 양자키분배(QKD, Quantum Key Distribution)로 구분
- 양자내성암호는 현대 암호 알고리즘[4]을 고도화하는 차세대 암호 기술이며, 양자키분배는 암호키 분배 과정에 양자역학을 접목한 양자 암호 기술
- 현대암호 중 공개키는 암호키의 보안을 강화하는 양자내성암호로 전환하고, 대칭키는 암호키의 길이를 확대함과 동시에 양자키분배를 신규 도입하여 동일한 키를 양측이 공유하는 암호키 분배 과정의 보안을 보장

〈그림 5〉 고전컴퓨터와 양자컴퓨터의 암호 체계



자료 : 산업자료 참고하여 당행 작성

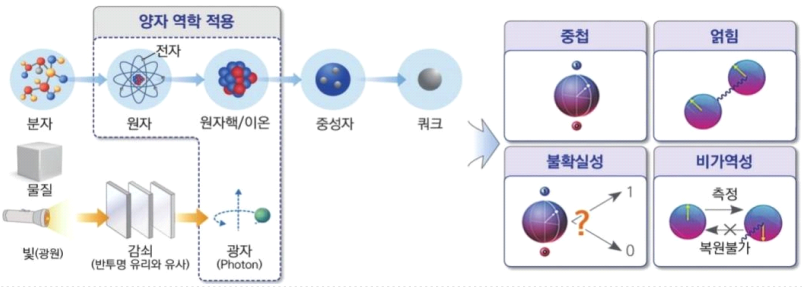
4) 알고리즘 : 문제 해결을 위해 컴퓨터가 이해할 수 있도록 순서대로 정리한 일련의 절차나 방법

〈참고 1〉 **양자키분배가 이용하는 양자역학의 주요 개념**

❑ 양자키분배는 빛을 구성하는 가장 작은 단위인 광자의 양자역학 특성을 이용

❍ 양자역학은 원자, 전자, 광자와 같이 미시 세계의 양자에서 유효한 물리 법칙
- 양자란 더 이상 쪼개질 수 없는 물리량의 최소 단위로, 물질에서는 원자와 전자, 빛에서는 광자 등이 존재
- 야구공처럼 일상의 거시 세계 물체에는 미래(움직임 등)를 정확히 예측하는 고전역학이 유효, 광자처럼 미시 세계 양자에는 미래를 확률로 설명하는 양자역학이 유효

양자역학의 적용 범위와 주요 특성



자료 : 국방기술진흥연구소(2023) "미래 전장의 게임체인저, 양자기술의 국방적용 방안 고찰"

❍ 양자키분배는 광자의 중첩·얽힘·불확정성·비가역성과 같은 양자역학 특성을 이용해 암호키의 보안(예측 불가능성)을 높이고 해커의 도청을 즉시 감지

양자역학 특성의 이용

특성	내용	양자키분배에서 이용
중첩	관측 전 여러 상태 가능성이 동시에 존재	상태 예측 불가를 암호키 난수생성에 활용
얽힘	멀리 떨어진 양자 쌍이 상관관계를 가짐	상관관계를 도청·간섭 여부 검증에 활용
불확정성	관측 전까지 상태는 미확정, 서로 관련된 상태는 동시에 정확하게 측정 불가	해커는 광자의 상태(수평·수직 또는 대각·역대각 편광[5])를 정확히 측정 불가
비가역성	관측 후에는 관측 전으로 복원 불가	해커는 관측 후 흔적 없이 복원 불가, 오류율 증가로 도청 시도 탐지 가능

자료 : 당행 작성

5) 편광 : 빛이나 전파같은 전자기파가 진행할 때, 진동 방향이 특정 방향으로 치우친 현상

2. 양자보안의 필요성

❑ 양자컴퓨터 고속 연산의 암호체계 위협과 HNDL(Harvest Now, Decrypt Later) 공격 감안시 양자보안은 시급

○ 양자컴퓨터 양자 알고리즘의 고속 연산능력은 현대 암호체계를 위협
- 그로버 알고리즘(Grover's Algorithm)은 대규모의 데이터베이스를 빠르게 탐색할 수 있어, 무차별 대입의 어려움을 이용한 대칭키 암호방식을 위협
- 쇼어 알고리즘(Shor's Algorithm)은 특정 수학문제를 현대 암호 알고리즘보다 빠르게 풀어내, 수학적 역산의 어려움을 이용한 공개키 암호방식을 무력화
- 다만, 양자컴퓨터는 큐비트 수의 양적 확장 등에서 아직 개발 단계 수준

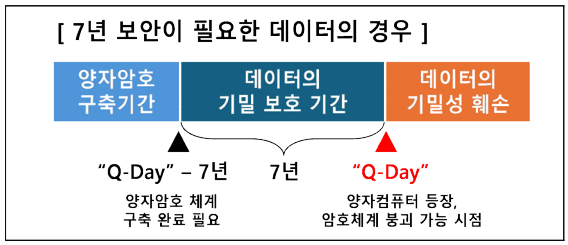
○ 고전컴퓨터로 풀 수 없는 암호화 데이터를 현시점에 탈취 및 수집하고 향후 양자컴퓨터로 해독하는 HNDL 공격은 현재 진행 중
- HNDL 공격은 즉각적인 피해를 주지는 않으나 국가 안보와 직결된 군사 기밀, 기업의 중장기 사업전략과 원천기술, 개인 의료정보나 금융이력과 같은 장기 가치를 지닌 정보에 치명적
- '30년으로 예상하는 Q-Day[6]와 데이터 기밀 보호 기간[7] 고려시 양자보안은 시급

〈표 2〉 양자 알고리즘이 위협하는 현대 암호

양자 알고리즘		현대 암호 알고리즘		
	특징		기반	방식
그로버	DB검색 속도향상	AES[8]	블록암호	대칭키
쇼어	수학문제 고속 풀이	RSA[9]	소인수분해	공개키
		ECC[10]	이산로그	

자료 : NIST IR 8105 등 자료, 당행 재구성

〈그림 6〉 양자보안의 시급성



자료 : 양자기술 국회 연속세미나(2026), 당행 재구성

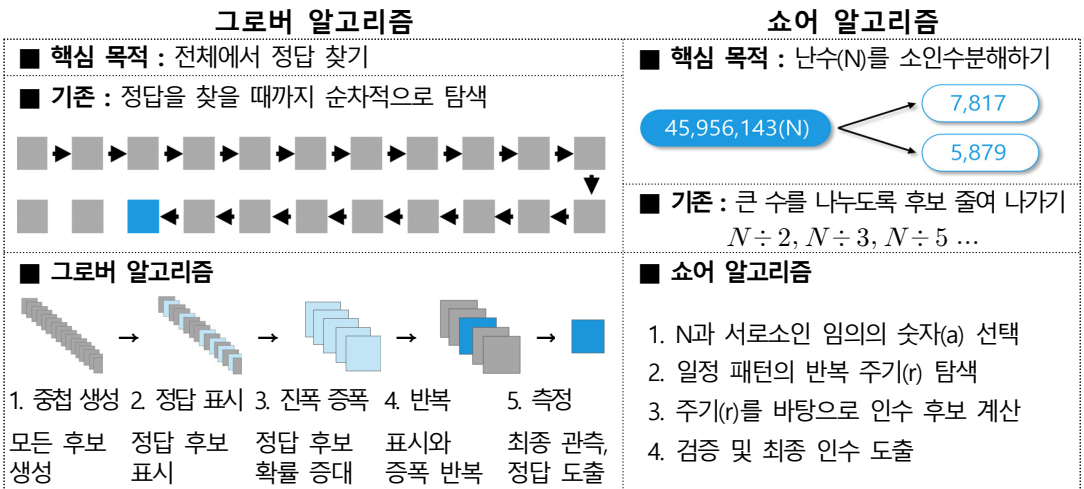
6) Q-Day : 양자컴퓨터가 현대 암호체계를 무력화하고 원장, 서명 등 모든 것의 위조가 가능한 시점
7) 기밀 보호 기간 : 특정 정보가 비인가자에게 노출되지 않도록 법적으로 기밀을 유지해야 하는 기간
8) AES(Advanced Encryption Standard) : 데이터를 블록(128비트 등과 같이 일정한 크기의 조각)으로 잘라 암호화하는 대칭키 암호 알고리즘
9) RSA(Rivest-Shamir-Adleman) : 큰 수의 소인수분해 어려움을 이용한 공개키 암호 알고리즘
10) ECC(Elliptic Curve Cryptography) : 이산로그(곱셈과 거듭제곱의 결과를 토대로 지수를 역산) 문제를 기반으로 하는 공개키 암호 알고리즘

〈참고 2〉 **양자컴퓨터 알고리즘의 원리와 위협 방식**

❑ 양자컴퓨터의 그로버알고리즘과 쇼어알고리즘은 각각 대칭키와 공개키 암호 방식을 위협

○ 그로버 알고리즘은 빠른 전수조사로 대칭키 암호의 보안 수준을 절반으로 약화
- 대칭키 암호는 난수생성기로 여러 자리의 예측 불가능한 비밀키를 생성
  · AES-128 알고리즘은 0과 1로 이루어진 128자리의 랜덤 비밀값을 생성, 해커가 2^{128}개의 가능한 모든 키를 하나씩 시도하면 탈취 가능하나, 고전컴퓨터에서는 엄청난 시간이 걸리므로 사실상 탈취가 불가
- AES-128의 보안성은 고전컴퓨터에서 2^{128} 수준, 양자컴퓨터에서 2^{64} 수준

○ 쇼어 알고리즘은 빠른 수학 문제풀이로 공개키 암호를 무력화
- 공개키 암호의 알고리즘인 RSA와 ECC는 소인수분해나 이산로그 등 어려운 수학문제를 기반으로 공개키와 개인키 한 쌍을 생성
  · RSA 알고리즘은 아주 큰 무작위의 소수 p, q를 곱한 N을 공개키에 사용, 해커가 공개된 N을 p, q로 역산하고 추가 가공하면 개인키를 탈취 가능하나, 고전컴퓨터에서는 수학적 역산이 어려워 사실상 탈취가 불가
- 공개키 암호 해독에 필요한 양자컴퓨터의 큐비트 수와 시간은 ECC-256이 10천개로 10일, RSA-2048이 100천개로 1개월 소요



자료 : 삼성증권(2026) "디지털 자산, 양자컴퓨터가 여는 금융 디지털자산 인프라 전환", 당행 재구성

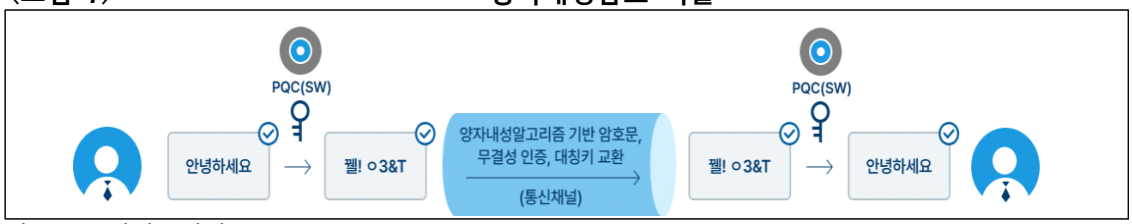
3. 양자 보안 기술

❑ 양자내성암호는 수학 난제 기반 암호 알고리즘 기술로, 호환성이 높지만 완벽한 보안은 어려움

○ 양자내성암호는 양자컴퓨터도 풀기 어려운 수학 문제인 격자[11], 코드[12], 해시[13] 등을 기반으로 한 공개키 암호 알고리즘 기술

- 기존 암호체계의 알고리즘을 업데이트하여 구현하는 소프트웨어 기술이며, 하나의 통신채널을 통해 인증·키교환·암호통신이 이루어짐

〈그림 7〉 양자내성암호 기술



자료 : 드림시큐리티

○ 기존 보안 시스템 및 통신·네트워크 인프라와 호환성이 높고 NIST(미국 국립표준기술연구소)를 중심으로 글로벌 표준화 진행 중

- 다만, 향후 양자컴퓨팅 기술이 고도화되어 모든 수학적 문제를 풀 수 있는 특이점 도달 시 안전성에 대한 본질적 한계 존재

· 표준 후보였던 SIKE 알고리즘은 '22년 인텔 CPU가 1시간 만에 해킹

〈표 3〉 NIST 양자내성암호 표준

구분	FIPS 203	FIPS 204	FIPS 205
알고리즘명	ML-KEM	ML-DSA	SLH-DSA
기반	격자	격자	해시
용도	키 교환	전자서명	전자서명

자료 : 산업 자료 종합, 당행 재구성

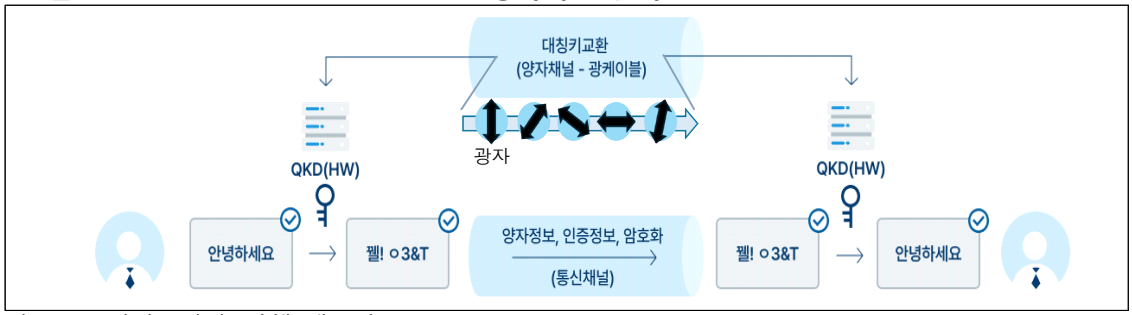
11) 격자 기반 암호 : 격자(lattice)라는 복잡한 수학적 구조에서 최단 벡터를 찾는 문제
12) 코드 기반 암호 : 메시지에 임의의 오류를 추가해, 수신자가 오류를 제거해야 메시지 복원 가능
13) 해시 기반 암호 : 입력 데이터의 크기와 상관없이 정해진 길이의 해시값을 반환하는 해시함수를 통해 나온 결과값에서 입력값으로 역산의 어려움을 이용

❑ 양자키분배는 양자역학 기반 암호키 분배 기술로, 이론상 완벽한 보안을 보장하나 인프라 구축이 어려움

○ 양자키분배는 광자의 양자 특성을 기반으로 통신 당사자 간 암호화에 사용할 대칭키를 안전하게 전달 및 분배하는 기술

- 암호화 데이터는 기존 통신채널을 통해 전송하고, 암호키는 정보가 담긴 단일 광자를 물리적으로 분리된 양자채널을 통해 전송하고 후처리하여 생성
- 광자(양자)를 탈취(관측)할 경우 광자 정보가 변하는 등 양자역학 특성에 의해 해킹을 원천적으로 차단

〈그림 8〉 양자키분배 기술



자료 : 드림시큐리티, 당행 재구성

○ 양자키분배에는 양자역학에 기반해 난수를 만드는 부품인 양자난수생성기(QRNG, Quantum Random Number Generator)가 필요

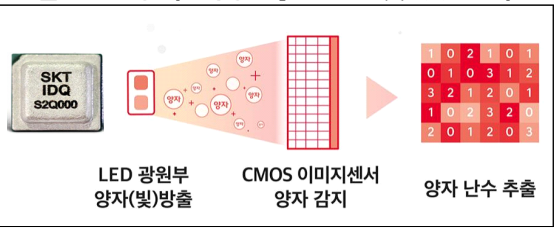
- 양자난수생성기는 광자 정보(편광 등), 방사성 동위원소의 붕괴 현상 등 자연에 기인한 무작위성을 물리적으로 추출해 예측이 불가한 진정난수 생성
- 기존 난수생성기는 수학적 알고리즘에 기인한 의사난수로, 패턴 예측이 가능

〈그림 9〉 양자키분배 장비



자료 : 과기부(2026) "2025 양자정보기술백서"

〈그림 10〉 광자 이용 QRNG 칩셋 및 원리



자료 : SK텔레콤 뉴스룸, 당행 재구성

〈참고 3〉 **양자키분배의 BB84 프로토콜**

❑ **양자키분배의 안전성은 프로토콜 설계에서 비롯되며, BB84 프로토콜[14]은 최초이자 현재 상용 시스템 대부분의 기반이 되는 표준 프로토콜**

○ BB84 프로토콜은 비트와 기저[15]의 조합으로 결정된 편광 정보를 단일 광자에 담아 암호키를 생성

① QRNG로 보내고자 하는 정보의 비트 수만큼 무작위 비트열(㉮~㉲)을 생성

② 송신자는 각 비트에 무작위로 기저(수직·수평, 대각·역대각)를 배정

③ 송신자는 편광 정보에 따라 편광된 광자를 만들고 양자 채널로 송신

· 사전 약속 정보에 따라, 비트와 기저의 조합으로 편광 정보를 결정

④ 수신자도 무작위 측정 기저를 생성하고 이를 이용해 수신한 광자를 관측

⑤ 수신자는 관측한 광자, 본인의 기저, 사전 약속 정보를 조합해 비트를 유추

⑥ 송·수신자간 전화 등 공개채널로 사용 기저 전체와 비트 일부(㉯㉱)를 공유

· 기저가 불일치 할 경우 정확도가 감소해 해당 비트는 암호키에 미사용

· 일부 비트는 도청 여부 판단을 위해 비교, 오류율이 높으면 도청으로 판단하고 지금까지 교환한 데이터로 암호키를 생성하지 않고 모두 폐기

⑦ 동일 기저 비트(㉯㉱㉰㉲) 중, 공유 비트(㉯㉱)를 제외한 나머지(㉰㉲)가 비밀키

BB84 프로토콜



구분			㉮	㉯	㉱	㉲	㉰	㉳	㉴
송신자	①	비트	1	0	0	1	1	0	1
	②	기저							
	③	편광 광자							
수신자	④	수신 광자[주]							
		기저							
	⑤	유추한 비트	0	0	0	1	1	0	1

주 : 중간 도청이 있을 경우 수신한 광자의 상태는 변하나, 현재 도청이 없다고 가정

자료 : 이순칠(2021) "퀀텀의세계" 등 산업 자료, 당행 재구성

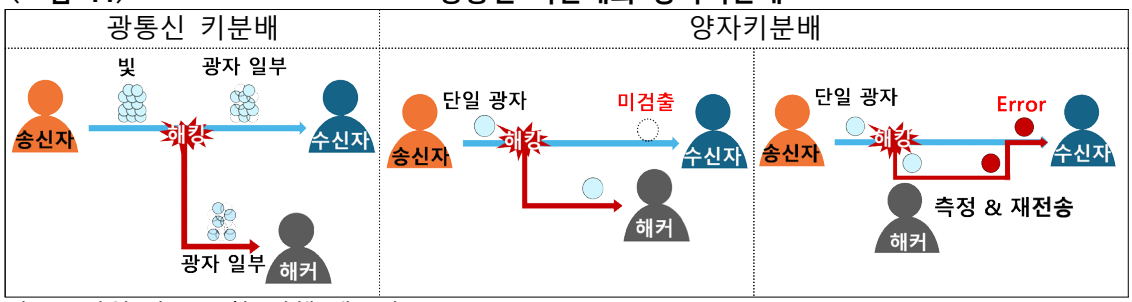
14) BB84 프로토콜 : '84년 제안자인 Bennett과 Brassard의 이름을 딴 최초의 양자키분배 프로토콜

15) 기저 : 양자상태(광자의 편광 등)를 측정하거나 부호화 하기 위해 사용하는 기준 측정 체계

○ 양자키분배는 단일 광자의 양자역학 특성을 이용해 해커의 탈취 정보를 무의미하게 하며, 도청의 즉각 감지가 가능

- 기존 광통신을 통한 키 분배는 빛(광자의 다발)을 이용해, 통신을 방해하지 않을 정도만 탈취해도 정보 획득이 가능하고 해킹 여부의 인지도 어려움
- 양자키분배는 단일 광자를 이용해, 광자 탈취시 정상적인 정보전송이 되지 않아 탈취된 정보는 의미가 없고 해커가 광자를 측정하고 재전송하면 불확정성과 복제불가능에 의해 오류가 증폭되어 해킹 사실을 감지

〈그림 11〉 광통신 키분배와 양자키분배

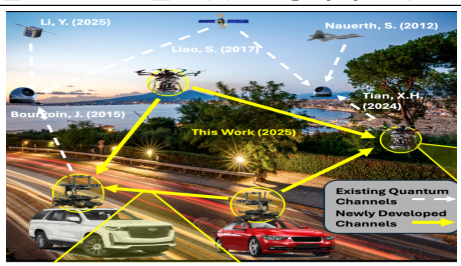


자료 : 산업 자료 종합, 당행 재구성

○ 양자키분배는 고가의 전용 장비와 광섬유 등 물리 네트워크가 필요해 인프라 구축이 복잡하고, 통신거리에 제약이 존재

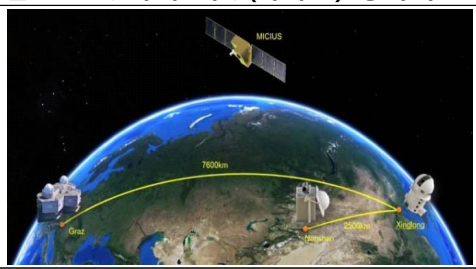
- 양자채널로 광섬유를 이용하는 유선방식은 광섬유 내부에서 빛의 손실로 인해 통신 가능 거리가 수백km에 제한되며, 양자의 얽힘 특성을 이용해 먼 곳까지 전달하는 양자중계기를 도입하면 해결이 가능하지만 아직 실험실 수준
- 양자채널로 자유공간(대기)을 이용하고 위성·드론 등과 결합한 무선방식은 초장거리도 가능하나, 기후 환경의 영향을 크게 받으며 기술 성숙도가 낮음

〈그림 12〉 드론을 이용한 양자키분배



자료 : 과기부(2026) "2025 양자정보기술백서"

〈그림 13〉 중국의 위성(묵자호) 양자키분배



자료 : PwC(2026) "Q-Day에 대비하라"

❑ 양자내성암호와 양자키분배는 대체재 관계가 아닌 다른 계층의 보완 관계로 두 기술을 하이브리드로 접목해 보안 강도의 극대화 가능

○ 양자내성암호는 대규모 트래픽 환경, 양자키분배는 절대 보안 구간에 적합
- 양자내성암호는 넓은 범위에 빠르고 유연하게 옮겨갈 수 있어 최근 상용화와 양자보안 확산을 주도 중이며, 클라우드, 금융거래, 블록체인, 공공데이터 등 대규모 트래픽 환경에 적합
- 양자키분배는 기술, 인프라, 비용 등의 제약이 있지만 이론상 완벽한 보안이 가능해 보안의 종착지로 예상하며, 군·외교, 위성통신, 국가기관망 등 절대 보안이 필요한 구간에 적합

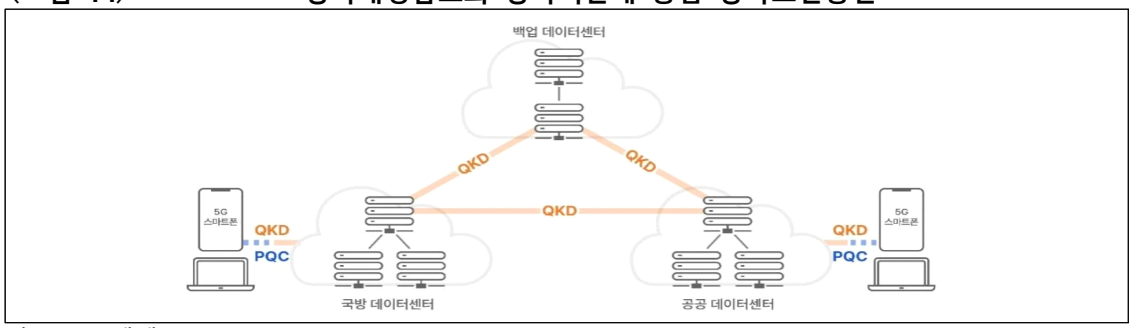
〈표 4〉 양자내성암호와 양자키분배 기술 비교

구분	양자내성암호	양자키분배
보안 기반	수학적 난이도(격자 등)	양자역학(불확정성, 복제불가 등)
공격 방식	양자컴퓨터로도 풀기 어려움	물리적으로 엿보는 것 자체가 불가
배포 방식	소프트웨어 업데이트	전용 하드웨어(광섬유·광자 장비)
비용 / 인프라	낮음 / 기존 인프라에 적용 가능	높음 / 별도 네트워크 필요
보안 보장 수준	계산상 안전	물리적으로 안전
대표 활용 분야	클라우드, 이메일, VPN 등	국가망, 금융망, 위성통신 등
한계점	미래 알고리즘의 공격 가능성	거리·채널 손실, 장비 결함

자료 : 백남정(2026) "AI 바이브코딩의 배신 AI 양자보안으로 막아라" 당행 재구성

○ 민감한 데이터를 저장하는 데이터센터에는 양자키분배를 적용, 무선 통신으로 외부 전송시 양자내성암호를 이용해 다중 방어 체계를 형성하고 전구간을 보호

〈그림 14〉 양자내성암호와 양자키분배 통합 양자보안통신



자료 : SK텔레콤 뉴스룸

Ⅲ. 국내외 동향

❑ Q-Day 도래 전, 주요국과 기업은 양자보안으로 전환을 위한 일정 수립과 기술 개발을 본격화

○ 현재 양자보안 기술을 개발하고 표준을 수립하는 단계로, 양자내성암호는 '30년초·중반까지 의무 전환 대상으로 채택했으나 양자키분배는 선택적 도입 대상
- 일부 글로벌 기업들은 시스템, 제품 등의 양자내성암호 전환 목표를 공식화

〈표 5〉 양자보안 도입 시기 전망

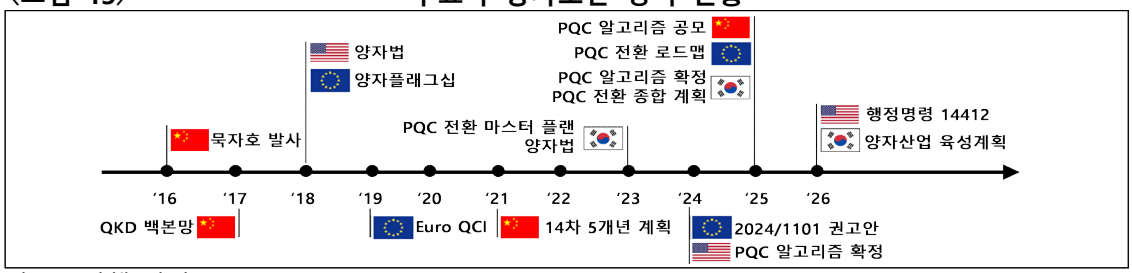
구분	현재	'30년	'35년 이후
양자컴퓨터	양자우위 달성, 양자컴퓨터 상용화	Q-Day 도래	
양자내성암호	표준제정 / 핵심인프라에 도입	도입 확산	
양자키분배	QKD망 구축·확산	PQC·QKD 병행	초고보안 영역 도입

자료 : PwC(2026) "Q-Day에 대비하라" 당행 재구성

❑ 미국은 양자내성암호, 중국은 양자키분배를 중심으로 주도권 경쟁을 벌이고 있으며, 기타 주요국 또한 독자적인 기술 확보에 주력

○ 미국은 양자키분배보다는 양자내성암호 중심의 전환 가속화 추진
- '18년「국가 양자 이니셔티브」제정으로 세계 최초의 국가 지원 체계를 구축
- NIST의 양자내성암호 알고리즘 표준 확정 이후, 최근 「행정명령 14412」을 통해 정부 핵심 시스템의 양자내성암호 전환 기한을 '31년으로 앞당겨 의무화
- 또한, 재무부는 '양자 준비 TF'를 출범해 금융권의 양자내성암호 전환을 가속

〈그림 15〉 주요국 양자보안 정책 현황

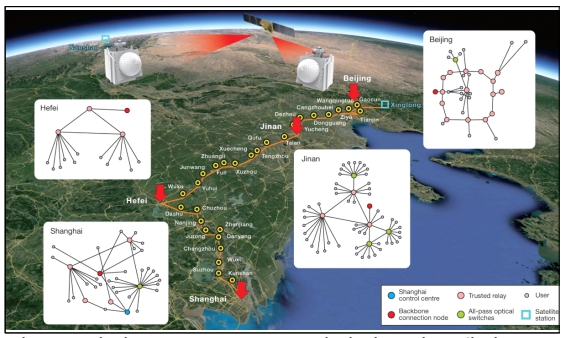


자료 : 당행 작성

○ 중국은 양자키분배의 선두 주자로 국가 주도로 대형 실증과 인프라를 구축
- 세계 최초의 양자통신위성 묵자호를 발사('16년)하고 베이징-상하이간 세계 최장 규모(2,000km)의 양자키분배 백본망[16]을 개통
- 아울러, '26년 중국과학기술대학교는 장치독립적 양자키분배(DI-QKD, Device Independent)[17]로 장거리 통신을 구현하는 등 양자키분배 기술을 선도
- 중국은「14차 5개년 계획('21~'25년)」에서 양자정보를 육성 분야로 선정하고, 현재 중국 자체 양자내성암호 표준 알고리즘을 공모하여 평가 중

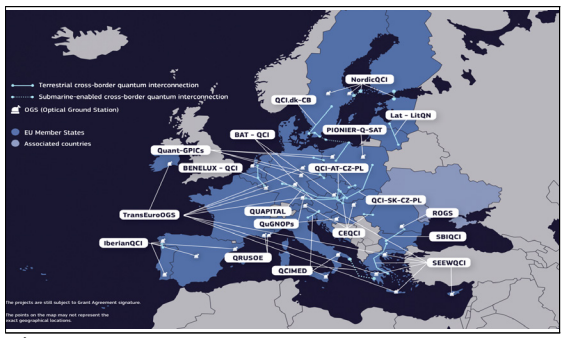
○ EU는 양자내성암호와 양자키분배의 균형 잡힌 전략을 추진하며 유럽을 하나로 묶는 공동 인프라 구축을 추진
- '18년 'EU 양자 플래그십'을 출범하여 10년간 양자기술 연구·사업화를 지원
- 양자키분배는 EuroQCI(Quantum Communication Infrastructure)에서 '30년까지 지상망과 위성망을 결합한 범유럽 양자통신 인프라를 구축할 계획이며, 현재 국가 간 지상망 연결을 진행 중으로 '27년 위성 발사 및 위성망 연결 예정
- 양자내성암호는「2024/1101」권고안과「양자내성암호 전환을 위한 공동이행 로드맵」을 통해 '35년까지 EU의 양자내성암호 전환을 완료할 예정

〈그림 16〉 중국 베이징-상하이 QKD 백본망



자료 : 과기부(2026) "2025 양자정보기술백서"

〈그림 17〉 EU QCI 지도



자료 : EU

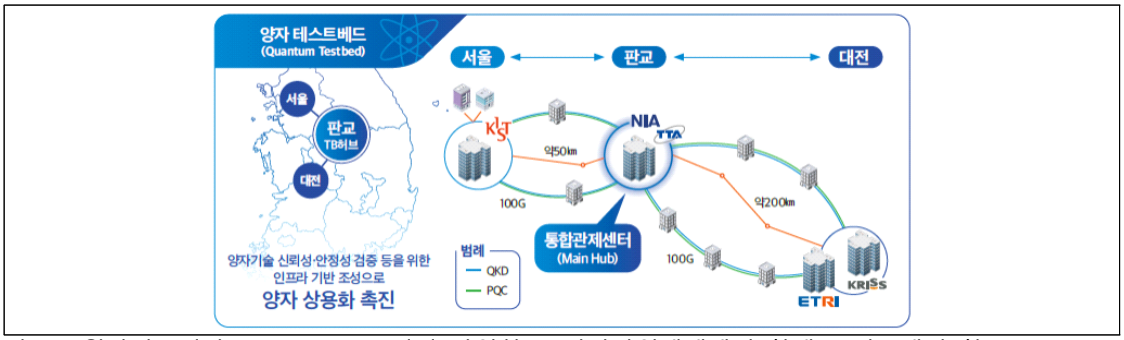
16) 백본망 : 저속의 여러 하위 망들을 서로 연결하거나 분산된 통신장치들을 통합하기 위한 최상위 통신 네트워크

17) DI-QKD : QKD는 이론적으로 해킹이 불가능하지만 실제 구현 과정에서 하드웨어적 허점을 노린 해킹에 취약할 수 있는 반면, DI-QKD는 불완전한 장비라도 완벽 보안 가능

○ 국내에서는 공공주도로 양자내성암호의 개발 및 실증을 진행하고, 자체 양자내성암호 표준화 작업을 추진

- '범국가 양자내성암호 전환 마스터플랜'을 통해 '35년까지 국내 양자내성암호 전환을 완료할 계획이며, 이를 위해 한국형 양자내성암호(KPQC)를 확정하여 표준화 작업을 진행 중
- 아울러, '양자과학기술 및 양자산업 육성에 관한 법률'을 제정해 국가차원의 양자산업의 육성과 양자보안 체계 구축 기반을 마련
- 공공주도로 양자 테스트베드를 개통해 양자 기술의 상용화를 지원 중이며, '제1차 양자과학기술 및 양자산업 육성 종합계획'에 따라 양자내성암호와 양자키분배 시범 전환 대상을 확대해 나갈 예정

〈그림 18〉 국내 개방형 양자 테스트베드 구성도



자료 : 월간인물기사(2025) "R&D를넘어 산업화로, 양자산업생태계의 확대로 기술패권 확보"

〈표 6〉 양자보안 분야 주요국 현황 비교

■ 기술력 우위

구분	미국	중국	EU	한국
양자내성 암호 (PQC)	표준화로 시장선도, PQC 도입가속화	PQC 행보 제한적, 미국 대비 열위	'30년 핵심인프라 PQC 도입목표	PQC특허 세계 1위, 공공주도 시범전환
양자 키분배 (QKD)	제한적 실증, 중국 대비 열위	위성 연계 대규모 실증, 세계최대 QKD망 구축, DI-QKD 등 고난도 기술구현	'27년 위성 연계 대규모 실증계획	유선망 초기실증, '30년 위성양자 암호통신 개발목표

자료 : PwC(2026) "Q-Day에 대비하라" 당행 재구성

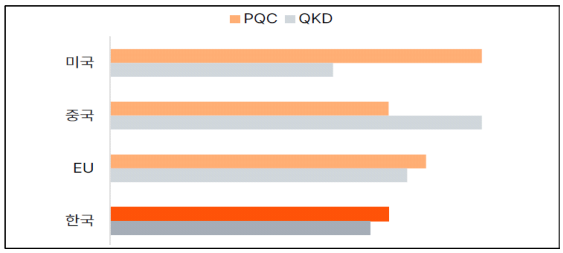
Ⅳ. 결론 및 시사점

❑ 양자보안 분야는 주요국과 기술격차가 작고 성장성이 높아, 한국에게 기회의 장

○ 국내 양자컴퓨터 기술은 미국과 중국 등 해외 주요국과 격차[18]가 큰 반면, 국내 양자 보안 기술은 미국, 중국 등 선도국을 추격 중

- 양자보안은 통신 인프라 위에서 암호 전환과 표준 대응 역량이 필요하고, 세계 최고 수준의 통신 인프라를 보유한 한국이 기술 상용화와 확산에 유리
  · 한국은 양자자내성암호 표준 특허 출원수 세계 1위를 차지하며 기술력 입증

〈그림 19〉 주요국 양자보안 경쟁력 비교



자료 : PwC(2026) "Q-Day에 대비하라"

〈표 7〉 국가별 양자내성암호 특허출원 현황

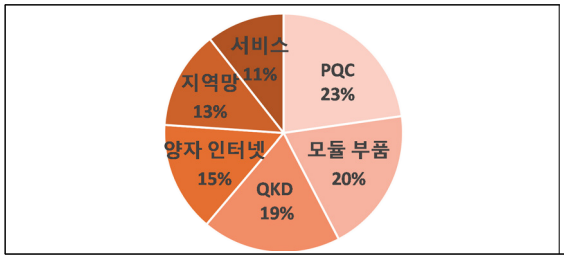
국가	출원수 (비중)	국가	출원수 (비중)
한국	101건 (46%)	중국	11건 (5%)
미국	48건 (22%)	프랑스	9건 (4%)
영국	27건 (12%)	일본	9건 (4%)
네덜란드	14건 (6%)	독일	2건 (1%)

자료 : 지식재산처(2026) 보도자료 당행 재구성

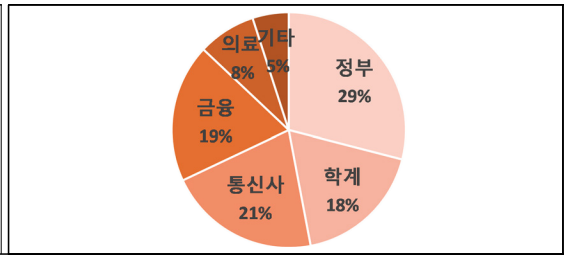
○ 양자보안 세계 시장규모는 '25년 15억불에서 '35년 128억불로 8.5배 고성장 전망

- '35년 분야별 시장에서 양자내성암호가 29억불, 양자키분배가 24억불을 차지하고, 고객별 시장에서 정부가 44억불, 통신사가 32억불, 금융기관이 29억불을 기록할 것으로 예상

〈그림 20〉 '35년 분야별 시장 비중



〈그림 21〉 '35년 고객별 시장 비중



자료 : McKinsey&Company(2026) "Quantum is almost here" 당행 재구성

18) 양자컴퓨터 큐비트 개발 현황 : 미국 IBM '23년 1,121개, 한국표준과학연구원 '24년 20개

❑ 양자보안 산업 육성에는 핵심기술 외에도 신뢰 인프라, 정부의 수요 창출 등이 필요

❍ 주요국은 산업화 초기단계인 양자기술을 전략기술로 분류하고 관리
- 양자기술은 미래 국가 기술 패권과 안보를 좌우할 핵심으로, 주요국에서는 전략기술로 분류하여 핵심 소재·부품·장비 등의 수출을 규제
- 양자보안 산업이 초기 단계임을 고려시, 서플라이체인 선점에 성공할 경우 자국 공급망 안정은 물론 해외 시장 개척까지 기대

❍ 양자보안은 핵심기술 외에도 서비스나 인증 같은 신뢰 인프라와 연계 필요
- 양자보안은 아직 표준·인증체계 등이 완전히 정착되지 않은 초기 산업
- 보안산업 특성상 핵심기술과 함께 표준·인증을 통한 신뢰성 입증이 중요하여, 암호화·장비 기술 등 요소기술을 넘어 응용서비스와 표준 및 인증까지 연결해 실제 도입 가능한 생태계를 구축하는 역량이 필요

❍ 정부는 국가주도의 인프라 구축으로 초기 수요 창출과 수출 기반 지원 필요
- 양자키분배 장비 1세트 가격은 수억원이며, 일정 거리마다 중계 장비도 필요하는 등 양자보안 인프라의 높은 구축 비용은 초기 수요창출의 최대 걸림돌
- 정부는 범국가적 양자보안 인프라를 구축하여 초기 수요를 창출하고, 실증 레퍼런스를 확보하여 국내 기업의 서플라이체인 선점과 수출 지원 필요

〈표 8〉 양자보안 산업의 4가지 주요 축

구분	주요 영역
기초 기술	양자 광원, 검출기
핵심 장비	QKD장비, QRNG칩
응용 서비스	금융·클라우드·에너지·국방 보안망
표준·인증	프로토콜·표준화·보안 검증

〈표 9〉 양자보안 산업이 직면한 과제

구분	문제
높은 비용	QKD 장비는 고가로 중소기업의 접근성이 낮음
다양한 표준	국가별·기업별 프로토콜이 달라 상호 연동성이 부족
인력 부족	양자 공학, 보안, 네트워크를 동시에 이해하는 인력 희소
정책과 인프라	인증·검증 체계, 법제화가 국가별로 상이

자료 : 백남정(2026) "AI 바이브코딩의 배신 AI 양자보안으로 막아라" 당행 재구성

참고문헌

[국문자료]

과학기술정보통신부(2023), “대한민국 양자과학기술 비전”
_____(2026), “2025 양자정보기술백서”
_____(2026), “제1차 양자과학기술 및 양자산업 육성 종합계획”
교보증권(2024), “양자키우기”
김종영(2023), “미래 전장의 게임체인저, 양자기술의 국방적용 방안 고찰”
딜로이트(2026), “양자컴퓨팅의 가능성을 현실의 가치로”
백남정·엄상윤·박나룡·박상민(2026), “AI 바이브코딩의 배신 AI 양자보안으로 막아라”
삼성증권(2026), “양자컴퓨터가 여는 금융·디지털 자산 인프라 전환”
삼일PwC경영연구원(2025), “큐비트의 마법, 상상을 계산하는 양자컴퓨터 혁명”
_____(2026), “Q-Day에 대비하라”
손민아·신성철(2023), “동형암호 기술과 활용 동향”
이순칠(2021), “퀀텀의 세계”
전경화·전삼현(2025), “양자내성암호 표준화 동향과 국내 금융암호 전환전략”
지식재산처(2026), “정부 최초로 온라인시스템에 한국형 양자내성암호 실증적용 추진”
최정운(2026), “QKD, PQC 등 양자암호 기술 최신 동향 및 발전 방향”
하나증권(2025), “4차산업 성장 이끌 양자암호통신 관련주”
한상욱(2018), “양자암호통신 개요 및 기술동향”

[영문자료]

Madelyn Cain(2026), “Shor’s algorithm is possible with as few as 10,000 reconfigurable atomic qubits”
McKinsey&Company(2025), “Quantum technology Monitor”
_____(2026), “Quantum is almost here”
OECD(2025), “Mapping the global quantum ecosystem”
Paul Webster(2026), “The Pinnacle Architecture: Reducing the cost of breaking RSA -2048 to 100 000 physical qubits using quantum LDPC codes”