Q-Day*에 대비하라:

양자기술이 가져올 보안 인프라 혁신

삼일PwC경영연구원 I Issue Brief
April 2026

* **Q-Day:** 양자컴퓨터가 원장 변경, 서명 위조, 통신 변조 등
기존 암호체계를 무력화하여 모든 것을 위조할 수 있는 시점을 의미

들어가며

양자컴퓨터 기술이 하루가 다르게 진일보하고 있다. 불과 1년 전에는 큐비트를 누가 더 많이 구현하는지가 기술 척도였지만 이제는 주요 양자기업들이 오류수정 칩을 선보이면서 누가 더 정확한지를 두고 경쟁 중이다. 양자컴퓨터가 현재의 컴퓨터를 유의미하게 능가하는 양자 우위의 시기도 그만큼 앞당겨지고 있다.

양자컴퓨터는 양자역학의 원리와 컴퓨터를 결합한 '꿈의 컴퓨터'다. 이 기술은 대규모 데이터 처리나 복잡한 계산에서 강력한 성능을 드러내며 여러 산업 분야에서 새로운 길을 개척할 것으로 기대된다. 그러나 양자컴퓨터가 가져올 혁신만큼이나 이로 인한 반작용 우려도 만만치 않다. 일각에서는 양자컴퓨터가 현재의 암호체계, 특히 공개키 기반 암호 인프라를 무력화하는 시점인 Q-Day가 2035년 내 도래할 확률이 50% 이상이라는 분석도 나온다.

이에 대한 대비책으로 등장한 개념이 양자보안이다. 양자보안은 양자컴퓨터 시대에 대응하여 보안체계를 강화하고 디지털 통신의 근간을 지키는 방패다. 구현 방식으로는 대표적으로 암호체계를 양자컴퓨터조차 해독하기 어려운 복잡한 알고리즘으로 업그레이드하는 방식, 양자역학의 성질을 역으로 이용해 암호체계의 근간을 바꾸는 방식이 있다. 이는 단지 이론에 머무는 연구주제가 아니라 주요국들을 중심으로 상용화가 추진 중인 당장의 현실이다. 미국에서는 상무부 산하 국립표준기술연구소(NIST)가 주요 기술 표준을 확정하여 발표했고, 중국은 일찌감치 위성을 활용해 세계 최장 수준의 양자암호 통신망을 구축했다. 이처럼 양자를 활용한 다양한 기술 분야 가운데 보안 영역이 가장 빠르게 상용화되고 있다.

본 보고서는 이러한 배경에서 양자보안의 중요성과 구체적 예시, 국내외 기업들의 개발 동향을 살펴보기 위해 작성됐다. 양자보안 시장 개화가 한국에 주는 시사점을 짚어보고 나아가야 할 방향을 제시한다.

Contents

I. 양자컴퓨터가 가져온 보안 위협 **03**

1. 2025 vs 2026, 1년 만에 달라진 양자컴퓨터의 위상 04
2. 양자컴퓨터 vs 기존 암호체계 07
3. 기술 발전의 필요조건: 보안 인프라 혁신 11

II. 양자보안, 모든 창을 막는 방패를 고안하다 **12**

1. 양자내성암호(PQC): 창이 뚫기 어려운 두꺼운 방패 14
2. 양자키분배(QKD): 창을 즉시 감지하는 방패 15
3. 시장 전망 및 활용 분야 17

III. 양자보안, 누가 어떻게 만들고 있나 **21**

1. 국가별 동향 22
2. 해외 기업 사례 24
3. 국내 기업 사례 26

IV. 시사점 및 제언 **29**

[Appendix] **34**

1. 양자역학 및 양자컴퓨터의 기본 개념 34
2. 양자통신 Value Chain 36
3. 양자통신 소재 · 부품 · 장비 목록 37

I

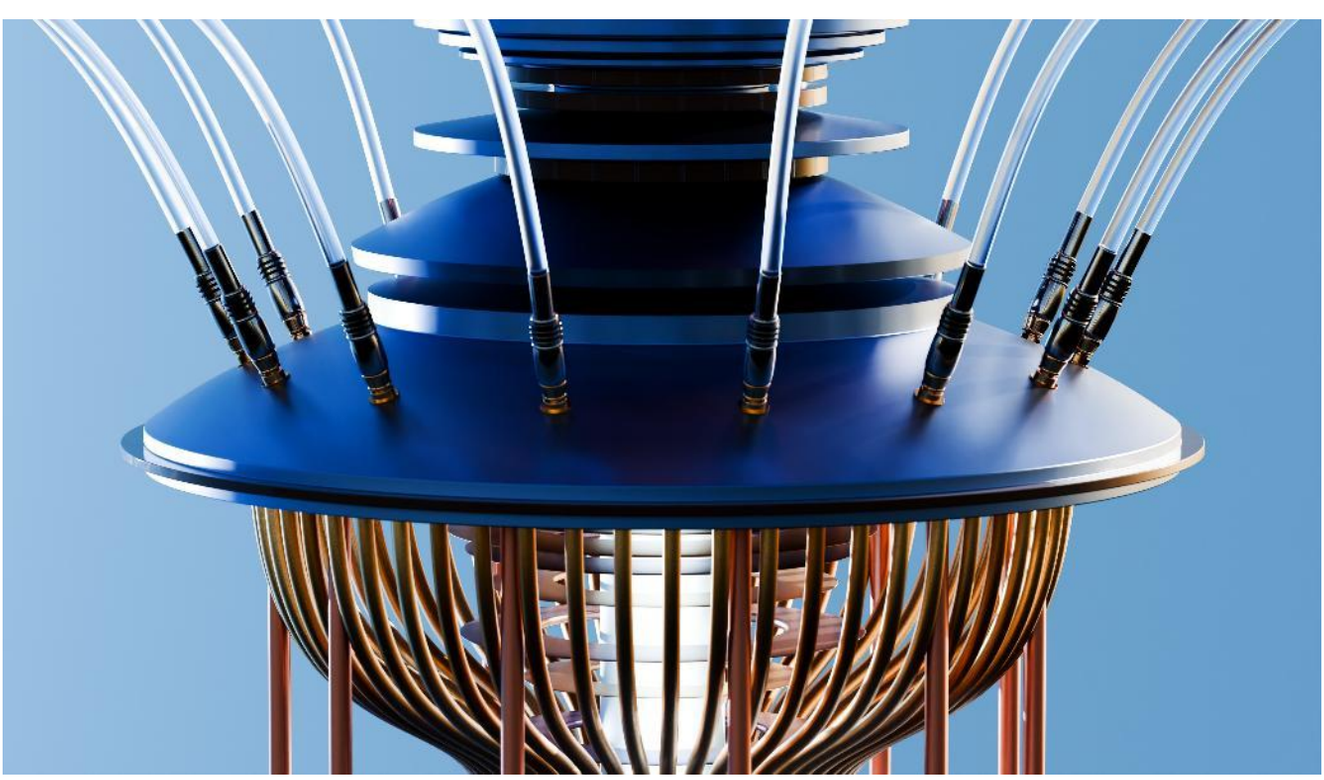
양자컴퓨터가 가져온 보안 위협

1. 2025 vs 2026, 1년 만에 달라진 양자컴퓨터의 위상

"유용한 양자컴퓨터 등장 시기와 관련하여 15년 후면 초기 단계, 30년 후면 후기 단계일 것이며, 20년 후라고 하면 많은 사람들이 믿을 것."

2025년 1월, 소비자 가전 전시회 CES(Consumer Electronics Show) 2025 현장에서 젠슨 황 NVIDIA CEO가 한 이 발언은 양자컴퓨터 업계에 찬물을 끼얹었다. 2024년 하반기부터 고공행진하던 주요 기업 IonQ, Rigetti Computing Inc 주가는 단 하루만에 각각 -39%, -45%의 낙폭을 기록했다. 젠슨 황 CEO가 두 달 후 해당 발언을 번복하며 사태를 무마했지만 이 때도 "양자컴퓨터 기업이 상장된 사실을 몰랐다"고 해명하며 양자기술 업계 자존심에 더 큰 상처를 남겼다.

그로부터 1년이 경과한 CES 2026 현장, 양자컴퓨팅 기술 및 관련 기업들의 위상은 눈에 띄게 달라졌다. 신설된 Foundry 공간에서는 NVIDIA 칩 기반 응용 기술 뿐 아니라 다양한 양자기술이 시연되며 산업 생태계 확장 속도를 드러냈다. 단순 개념 제시를 넘어 실제 작동하는 솔루션의 시연은 양자기술이 막연히 먼 미래만 바라보는 연구 주제에서 산업 현장의 실질적 도구가 되고 있음을 입증했다.



CES 2026에 참가한 주요 양자컴퓨터 기업 예시

구분	주요 내용
D-Wave Quantum	• 여러 제약조건이 존재하는 환경에서도 최적화와 방대한 데이터 처리에 효과적인 양자 어닐링(*) 방식의 양자 · 고전 컴퓨팅 결합 솔루션 활용 • 클라우드 기반 환경을 통해 제약조건을 가진 최적화 문제에 양자기술을 적용할 수 있도록 함으로써 실제 산업 문제 해결에 대한 접근성을 높임 • CES 현장에서 제조, 공급망, 통신 등 다양한 산업 분야의 실제 고객 사례를 통해 기술 적용 효과 시연
SuperQ	• ChatQLM은 사용자가 자연어로 질문을 입력하면, 양자컴퓨팅과 슈퍼컴퓨팅, 고급 최적화 기술을 결합해 의사결정에 필요한 분석 결과를 제공하는 양자 AI 기반 애플리케이션 • QLM(Quantum Learning Machine) 기반 하이브리드 연산 구조를 통해, 문제의 성격에 따라 슈퍼컴퓨터, 양자 어닐링, 게이트 기반 양자컴퓨터 등 다양한 연산 자원 중 최적의 계산 방식을 자동으로 선택해 결과를 도출 • 복잡한 양자기술에 대한 전문 지식이나 별도의 설정 없이도 사용할 수 있도록 설계되어, 양자기술을 연구 · 전문 인력의 영역에서 벗어나 일반 사용자도 활용 가능한 응용 플랫폼으로서의 방향성 제시
Quantum Computing Inc.	• 실온 · 저전력 환경에서 작동 가능한 광자 기반 양자컴퓨터를 개발하고 있으며, 양자광학과 집적 포토닉스 기술을 활용해 데이터센터나 산업 현장에서도 운용 가능한 양자 시스템 구현을 목표로 하고 있음 • CES Foundry에서 금융 모델링, AI 학습, 드론 경로 최적화 등 실제 산업 문제를 대상으로 한 데모를 통해, 광자 기반 양자컴퓨팅의 빠른 판단과 효율적인 최적화 가능성 입증 • 포토닉 기반 양자 시스템의 개발 및 상용화 가속화 전략 제시

(*) 양자역학 성질을 활용하여 수많은 경우의 수 중 최적값(최저 에너지 상태)을 찾아내는 방식. 어닐링 기법은 산봉우리가 있는 지역에 내린 비가 중력에 의해 낮은 곳으로 고이는 현상을 통해 가장 낮은 위치(최적값)를 찾는 방법으로 이해할 수 있음. 한편, 양자의 세계에서는 양자 중첩의 영향으로 입자가 에너지 장벽을 넘어서는 양자 터널링 현상이 나타남. 이 특성을 어닐링 기법에 적용해 진정한 최적값 탐색 가능

자료: 삼일PwC경영연구원

CES 2026에 참가한 주요 양자컴퓨터 기업 부스

자료: 삼일PwC경영연구원

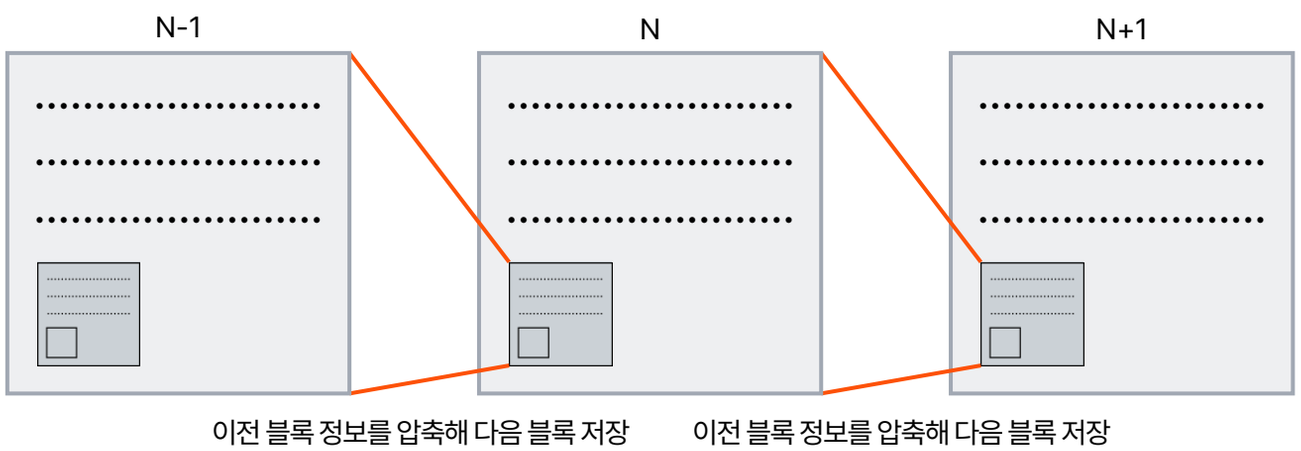
글로벌 빅테크를 이끄는 주요 인사들도 양자컴퓨터의 빠른 상용화 전망에 힘을 보태고 있다. 2026년 2월 줄피 알람 Microsoft 양자 부문 부사장은 2029년에 양자 시스템이 데이터센터에 도입되어 고전 컴퓨터로는 처리 불가능한 계산을 수행할 것으로 내다봤다. 순다르 피차이 Google CEO는 2025년 10월 Salesforce의 IT 연례 행사 Dreamforce 2025에 참석해 양자컴퓨터의 잠재력에 대해 긍정적으로 평가하며, 수년 내에 상용화 가능한 대규모 양자컴퓨터 출시 계획을 밝혔다. 투자은행 UBS는 고전 컴퓨터가 현실적으로 풀 수 없는 문제를 양자컴퓨터가 해결하는 단계(이를 '양자 우위'라 일컫는다.)가 2030년대 초에 달성될 것으로 전망했다. 멀게만 느껴졌던 양자기술은 생각보다 빠르게, 연구실을 벗어나 구체적으로 윤곽을 드러내고 있다.

2. 양자컴퓨터 vs 기존 암호체계

2024년 말 Google은 현재의 슈퍼컴퓨터로 10의 25제곱 년을 걸려야 풀 수 있는 계산을 자체 개발 양자 칩 Willow를 통해 단 몇 분 만에 해결할 수 있다고 발표했다. 이러한 압도적 연산 능력은 기존까지 해결할 수 없었던 수많은 난제들을 새로운 방식으로 풀 수 있는 잠재력을 의미한다. 이와 함께 단골처럼 등장하는 논쟁거리가 있다. 비트코인의 붕괴 가능성이다. 양자컴퓨터가 상용화될 만큼 기술 고도화가 이루어지면 비트코인의 블록체인 알고리즘이 해킹 · 조작될 수 있다는 주장이다.

블록체인에서 말하는 블록이란 일정 시간 주기로 생성되는 데이터 저장 단위이다. 거래 기록을 모아 블록을 만들어 신뢰성을 검증하면서 이전 블록에 연결하여 블록체인 형태를 이룬다. 즉, 블록체인은 기존 신규 블록이 연결되며 시간의 흐름에 따라 수직적으로 연결되는 기술이다.

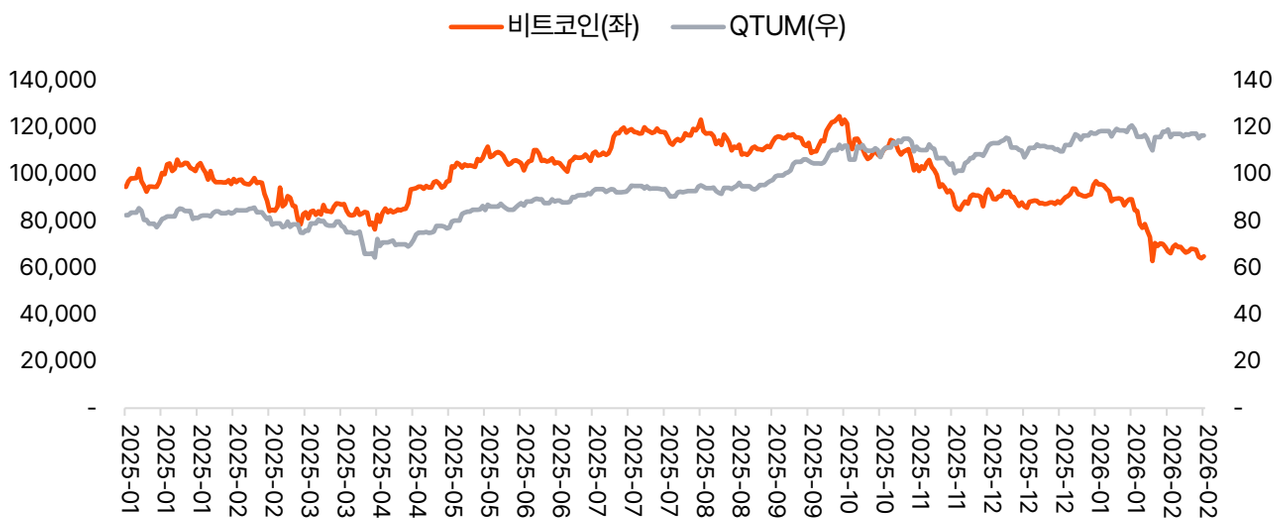
블록체인의 구조



자료: 삼일PwC경영연구원

비트코인의 거래 장부는 블록체인 기술을 바탕으로 여러 사용자들의 서버에 분산 · 저장되기 때문에 해킹이 불가능에 가깝다. 모든 정보가 외부에 공개는 되어 있지만 이 정보를 조작하기는 너무나 어려운 구조다. 그러나 일각에서는 양자컴퓨터가 가져올 혁신이 비트코인의 근간을 파괴할 수 있지 않겠냐는 우려가 나온다.

비트코인 · 양자컴퓨팅 ETF(Defiance Quantum ETF, QTUM) 가격 추이 (단위: 달러)



(*) 유의: 상기 가격 추이는 단순 참고 목적. 비트코인 가격은 반감기, 금리 전망, 지정학적 리스크 등 복합적인 요소에 의해 등락을 거듭하고 있으며 최근 하락세의 원인이 양자컴퓨터에 있다고 보기는 어려움

자료: Investing.com

비트코인이 자주 인용될 뿐이지 이는 비단 비트코인에 국한되는 문제가 아니다. 다른 암호체계보다도 현재의 공개키 기반 암호 알고리즘 환경에 전반적으로 문제가 발생한다. 우리가 일상에서 누리는 암호화된 금융 · 통신 인프라의 해킹 위험이 따라붙는, 이른바 Q-Day가 도래할 수 있다.

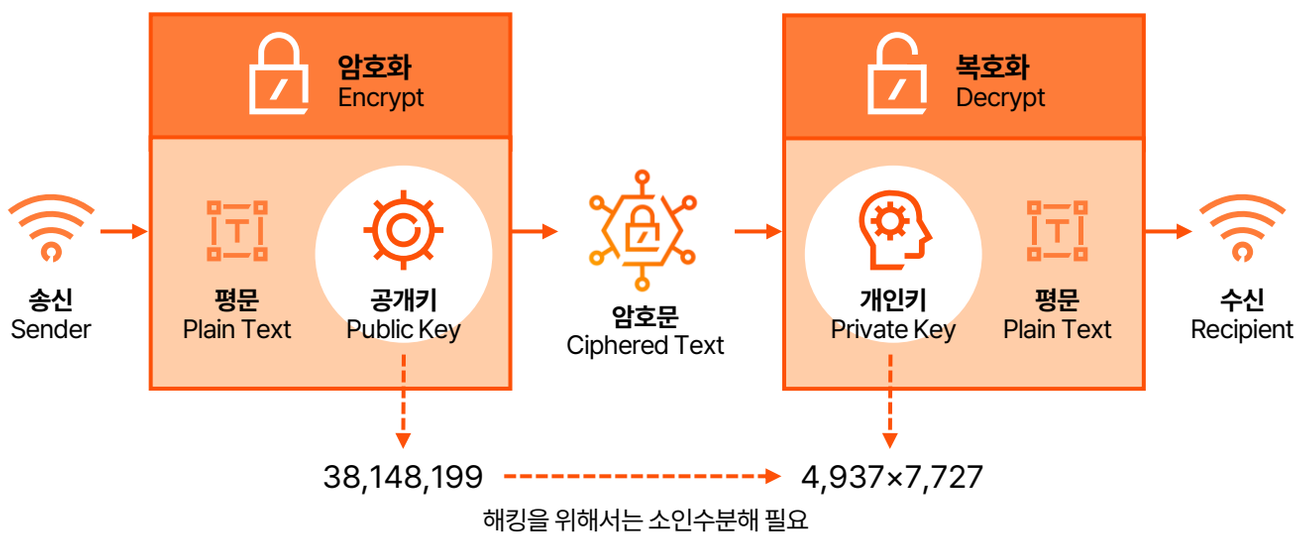
※ Q-Day

양자컴퓨터가 기존 암호체계를 실질적으로 무너뜨릴 수 있게 되는 날.
즉, 양자컴퓨터가 원장 변경, 서명 위조, 통신 변조 등 모든 것을 위조할 수 있는 시점을 의미. Q-Day는 공식적으로 약자가 정해진 용어는 아니지만 Q는 맥락상 Quantum을 가리키는 상징적인 표현

현재 웹사이트 접속, 인터넷 뱅킹, 데이터 전송, 여권 등에 폭넓게 쓰이는 가장 보편화된 암호화 방식은 RSA이다. 1977년 이를 고안한 3명의 수학자(Rivest, Shamir, Adleman)의 이름을 딴 암호체계로 매우 큰 두 개의 소수를 이용해 해독이 어려운 암호를 만드는 방식이다.

소수(Prime Number)란 1과 자신 외 다른 숫자로 나누어 떨어지지 않는 자연수로 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 등으로 이어진다. 이러한 소수끼리 곱한 값을 암호화한다면 외부에서 이를 복호화하기 위해서는 다시 소인수분해를 해야 한다. 암호화된 값이 10이라면 2×5로 간단히 답을 찾을 수 있지만 세자릿수 소수인 199와 277을 곱한 55,123만 보더라도 역산이 쉽지 않다. 두 소수의 자릿수가 각각 10자리 이상으로 커지면 두 수의 곱을 소인수분해하는데 슈퍼컴퓨터로도 수만년이 소요된다고 알려져 있다.

RSA 암호체계의 작동 방식



자료: Encryption Consulting, 삼일PwC경영연구원

그러나 아무리 난해한 소인수분해라도 슈퍼컴퓨터 대비 수만배 이상의 연산 성능을 탑재한 양자컴퓨터 앞에서는 안전성을 담보하기 어렵다. 이는 단지 기우가 아니라 1994년에 이미 입증된 사실이다. MIT 수학자 피터 쇼어는 양자중첩을 이용해 복잡한 소인수분해도 충분히 계산 가능함을 보이며 RSA의 한계를 드러냈다. 그러나 당시만 하더라도 양자컴퓨터 상용화는 별나라만큼이나 먼 이야기로 치부되었으므로 RSA의 입지에는 큰 영향을 미치지 못한 것으로 추측된다.

피터 쇼어의 연구 이후 30년 이상 경과한 현 시점, 아직 양자컴퓨터가 공개키 암호체계를 무력화할 수준에 도달하지는 못했다. 그러나 늦기 전에 이에 대응할 새로운 보안 시스템이 필요하다는 공감대는 충분히 형성됐다. 글로벌 시장조사업체 Gartner는 2026년 주요 사이버 보안 트렌드를 제시하며, 그 중 하나로 양자컴퓨터 발전에 따른 암호화 전환의 필요성을 강조했다.

2026년 주요 사이버 보안 트렌드

에이전틱 AI, 사이버보안 관리 · 감독 필요성 확대	• 생성형 AI를 넘어 자율적으로 작업을 수행하는 AI 에이전트 도입이 확산되면서, 이를 감독하고 통제할 수 있는 새로운 보안 체계 필요
글로벌 규제 변동성이 사이버 복원력 강화 촉진	• 지정학적 불안과 규제 변화가 기업 경영의 위협 요소가 되면서 단순 방어를 넘어 공격받아도 즉시 복구할 수 있는 '사이버 복원력'이 중요
포스트 양자컴퓨팅, 실행 단계로 진입	• 양자컴퓨터 발전으로 현재의 암호화 방식은 2030년까지 안전성을 확보하기 어렵다는 우려 • "지금 데이터를 수집하고 나중에 복호화하는" HNDL 공격 피해를 막기 위해 포스트 양자 암호화 전환 필요
AI 에이전트에 맞춰 진화하는 IAM(신원 및 접근 관리)	• AI 에이전트 등장으로 신원 등록, 거버넌스, 자격 증명 자동화, 권한 부여 전반에 구조적 전환 필요
AI 기반 SOC(보안운영센터) 솔루션이 운영 관행 불안정화	• AI를 이용한 위협 탐지 및 케이스 분류가 고도화됨과 동시에 AI 툴 도입에 따른 비용 및 운영 복잡성 증가
생성형 AI가 기존 사이버보안 인식 전략 무력화	• 기존의 보안 인식 교육은 더 이상 효과가 없음 • 57% 이상의 직원이 개인 계정의 생성형 AI를 업무에 활용하고 민감 정보를 입력하고 있어 AI 특화 보안 교육 필요

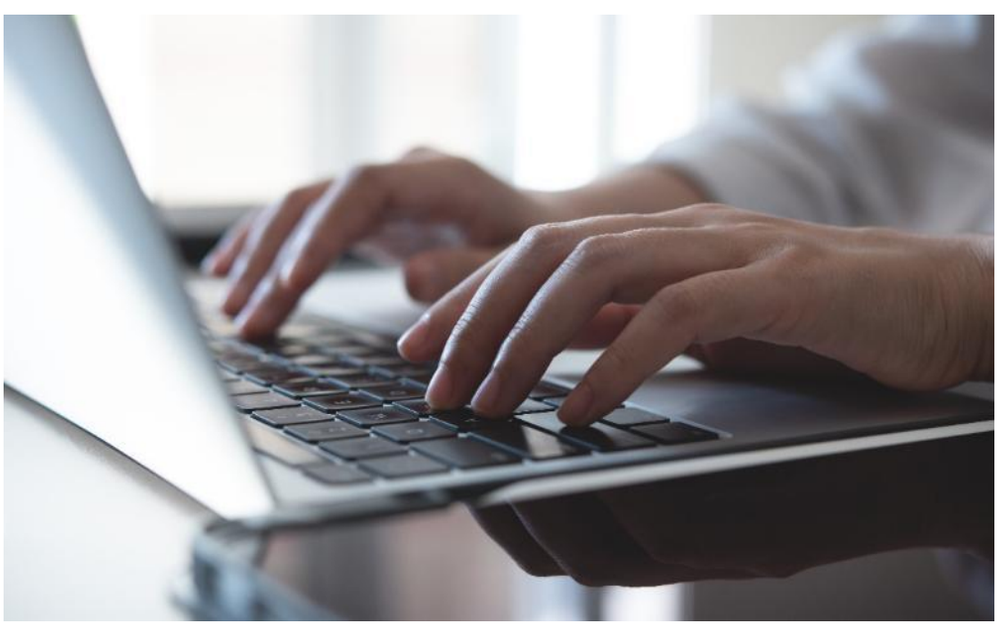
자료: Gartner(2026.02)

특히 Gartner는 지금 암호화된 데이터를 수집해 보관하고 있다가, 나중에 양자컴퓨터 등 고성능 해킹 기술이 등장하면 이를 복호화하는 HNDL(Harvest Now, Decrypt Later) 공격 피해 가능성을 꼬집었다. 양자컴퓨터 상용화까지 아직 시간이 남았다고 대비를 늦출 게 아니라 지금 당장 데이터를 보호할 수 있는 새로운 암호체계 도입이 시급한 이유다.

3. 기술 발전의 필요조건: 보안 인프라 혁신

예측된 위기는 위기가 아니라는 말이 있다. 보안 위기감이 커지는 만큼 대비책도 부상하고 있다. 양자컴퓨터 시대에 대응하여 전체 보안 체계를 강화하는, 이른바 '양자보안'이다. 마크 베니오프 Salesforce CEO는 양자컴퓨터의 보안 체계 위협과 관련하여 이러한 위험이 새로운 기회(보안업계의 혁신)를 창출할 것으로 전망했다. 순다르 피차이 Google CEO도 현재의 암호체계를 대신할 새로운 암호, 양자내성 암호의 필요성을 강조했다. Google은 Q-Day에 대비하기 위한 내부 준비 시한을 2029년으로 설정하며 업계 대응을 촉구하기도 했다.

양자보안은 양자컴퓨터라는 창에 맞설 방패로 각광받는 분야이지만 양자컴퓨터를 차치하더라도 그 필요성은 여전하다. AI 대전환의 격동기를 맞아 보안의 중요도는 거듭 높아지고 있다. AI가 기본 인프라로서 개인과 기업활동 저변에 깔리고, 더 많은 정보와 권한을 갖는 에이전트, 초지능 단계로 나아가려면 보안 · 안전장치 분야의 발전도 마찬가지로 가속화되어야 한다. 보안이 취약하면 누구도 AI 에이전트를 마음 놓고 쓸 수 없다. 누구도 자율주행차 · 도심항공교통이 해킹으로부터 안전하다고 장담할 수 없다. 불안해서 쓰지 못하는 기술은 무용지물이다. 따라서 기술 발전과 확산의 필요조건으로 보안 인프라 혁신이 전제되어야 한다. 양자보안이 그 해답이 될 수 있다.



II

양자보안,
모든 창을 막는 방패를 고안하다

전술한 바와 같이 양자보안은 양자컴퓨터 시대에 대비해 보안체계 전반을 강화하는 개념이다. 현재 이를 구현하는 방식은 대표적으로 양자내성암호(Post Quantum Cryptography, PQC)와 양자키분배(Quantum Key Distribution, QKD)가 있다. PQC는 양자컴퓨터조차 풀기 어려운 복잡한 계산에 의존하는 암호체계인 반면, QKD는 계산이 아닌 양자역학 물리법칙에 기반하여 해킹 시도를 즉각 알아차리는 양자암호통신이다. 비유하자면 PQC는 창(양자컴퓨터 공격)에 더 잘 버틸 수 있도록 방패를 더 두껍게 만드는 방식이며, QKD는 창의 성질을 활용해 공격을 즉시 감지하는 완전히 새로운 방패다. 두 기술은 대체재 관계에 있기보다는 서로 다른 계층적 보안체계를 구현하는 보완적 관계로 볼 수 있다.

암호체계 유형별 비교

구분	일반 암호(RSA 등)	양자내성암호(PQC)	양자키분배(QKD)
기반	소인수분해 등 복잡한 수학적 계산	양자컴퓨터가 풀기 어려운 수학적 계산	양자역학 물리법칙
구현 방식	소프트웨어 업데이트	알고리즘 업데이트	광 통신 등 특수 장비
특징	• 양자컴퓨터에 취약	• 국제 표준화 진행 중 • 양자컴퓨터 안전성 불확실 • 빠른 적용 가능	• 물리적 보안, 통신 인프라 보완 필요 • 물리법칙을 통해 무조건적인 안전성 구현 가능

자료: 언론종합

1. 양자내성암호(PQC): 창이 뚫기 어려운 두꺼운 방패

먼저 PQC부터 알아본다. PQC는 양자컴퓨터가 상용화되어도 풀기 어려운 복잡한 수학적 문제로 안전성을 높인다. 앞선 RSA 등 현재의 공개키 암호체계가 소인수분해를 이용한다면 PQC는 이보다 난해한 격자나 해시(Hash), 다항식의 개념을 활용해 암호를 생성한다. 기존의 보안 시스템, 통신 · 네트워크 인프라를 전면 교체하지 않고 수학적 알고리즘을 업그레이드하는 방식으로 구현할 수 있어 빠른 적용이 가능하다는 게 장점이다.

PQC 도입을 권장하고 있는 미국은 상무부 산하 국립표준기술연구소(NIST)를 중심으로 2016년부터 PQC 표준화 프로젝트를 추진해왔다. NIST는 국제 공모와 검증 과정을 거쳐 2024년 8월, 양자컴퓨터 공격으로부터 안전하도록 설계된 세 가지 공식 표준(Federal Information Processing Standard, FIPS)을 발표했다. 표준이 확정되면서 하드웨어에 PQC 탑재가 보편화(Security by Design)되려는 조짐도 나타난다.

NIST PQC 1차 표준

구분	FIPS 203	FIPS 204	FIPS 205
표준명	ML-KEM	ML-DSA	SLH-DSA
기반	**모듈 격자**	**모듈 격자**	**해시**
용도	키 캡슐화, 키 교환	전자서명	전자서명

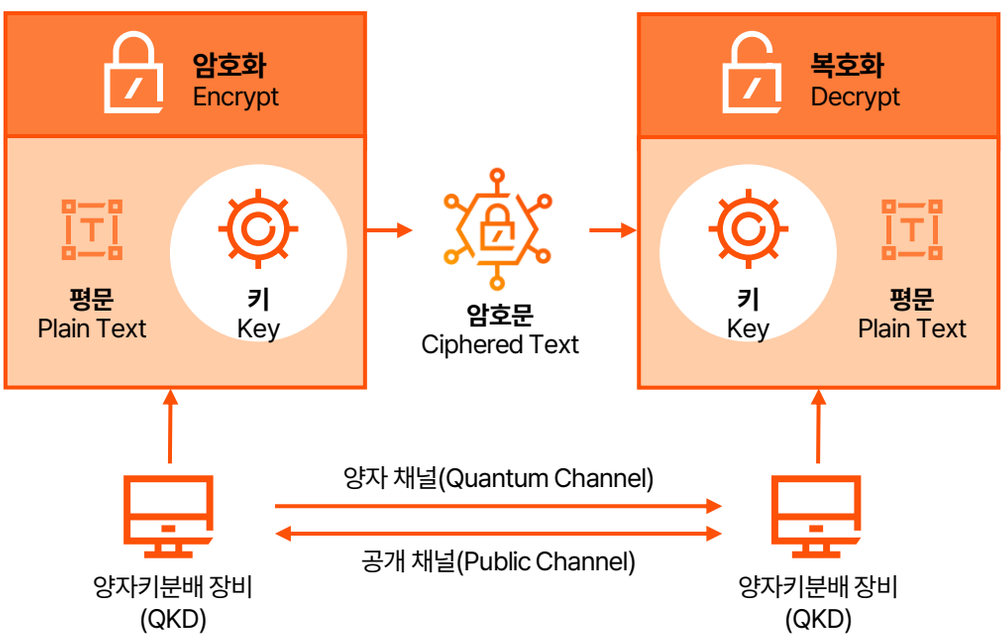
자료: NIST

기존 인프라와 호환성이 높고 도입이 용이한 만큼 업계 실증도 활발하지만 본질적 한계는 있다. 격자, 해시 등 복잡한 구조가 당장은 안전을 담보할 수 있어도 양자컴퓨터라고 가만 있으리란 법이 없다. 향후 컴퓨팅 기술이 더욱 고도화돼 양자컴퓨터가 풀기 어려운 수학적 계산이 사실상 사라지는 특이점에 도달하게 되면 PQC 방어망도 안전지대가 아니다. 한때 PQC 표준 후보 중 하나였던 SIKE(Supersingular Isogeny Key Encapsulation) 암호 알고리즘은 2022년 Intel 싱글 코어 CPU에 1시간 만에 해킹되며 고배를 마셨다. 현재 확정된 PQC 표준이라고 해서 안심할 수 없는 이유다.

2. 양자키분배(QKD): 창을 즉시 감지하는 방패

PQC가 기존 암호체계를 더 정교하게 업그레이드하는 방식인 데 비해 QKD는 양자역학의 물리법칙을 이용해 아예 판을 새로 짠다. 구체적으로 중첩과 불확정성 원리, 그리고 관측되는 즉시 상태가 확정되는 양자의 고유 성질을 이용한다. 송신자가 데이터를 암호화하는 키를 양자 상태로 전송함으로써 수신자도 암호키를 양자 상태로 전송받는다. 중간에 제3자가 이를 가로채려 한다면 제3자의 관측에 의해 암호키의 양자 상태가 즉시 변하므로 해킹 시도가 100% 감지되고 암호키는 폐기된다. 양자 상태의 변동 여부로 모든 도청 · 감청 · 해킹 시도를 알아챌 수 있으므로 완벽한 방어망이다. 다만, 암호체계의 패러다임을 바꾸는 기술인 만큼 현재의 보안 시스템과 호환성이 낮고 PQC 대비 구현이 어렵다.

QKD 암호체계의 작동 방식



자료: Centre for Development of Telematics, 삼일PwC경영연구원

QKD는 구현 방법에 따라 유선과 무선으로 구분된다. 유선 QKD는 광 섬유 선로를 전송 채널로 이용한다. 광 섬유를 통해 전송되는 신호 감쇄를 최소화하면서 통신 거리를 확장하는 것이 관건이다. 국내 주요 통신기업들이 유선 QKD 상용화 개발에 집중하며 기술 선도국들을 추격하고 있다.

무선 QKD는 물리적 매개체 없이 대기 환경을 채널로 이용하여 신호를 전송한다. 인공위성을 활용해 수백km 떨어진 지상 간 장거리 양자 통신을 구현하는 위성 QKD가 대표적이다. 날씨의 영향에 민감하고 거리가 길어질수록 신호가 분산 · 손실될 가능성이 있으므로 수신 효율을 높여야 하는 과제를 안고 있다.

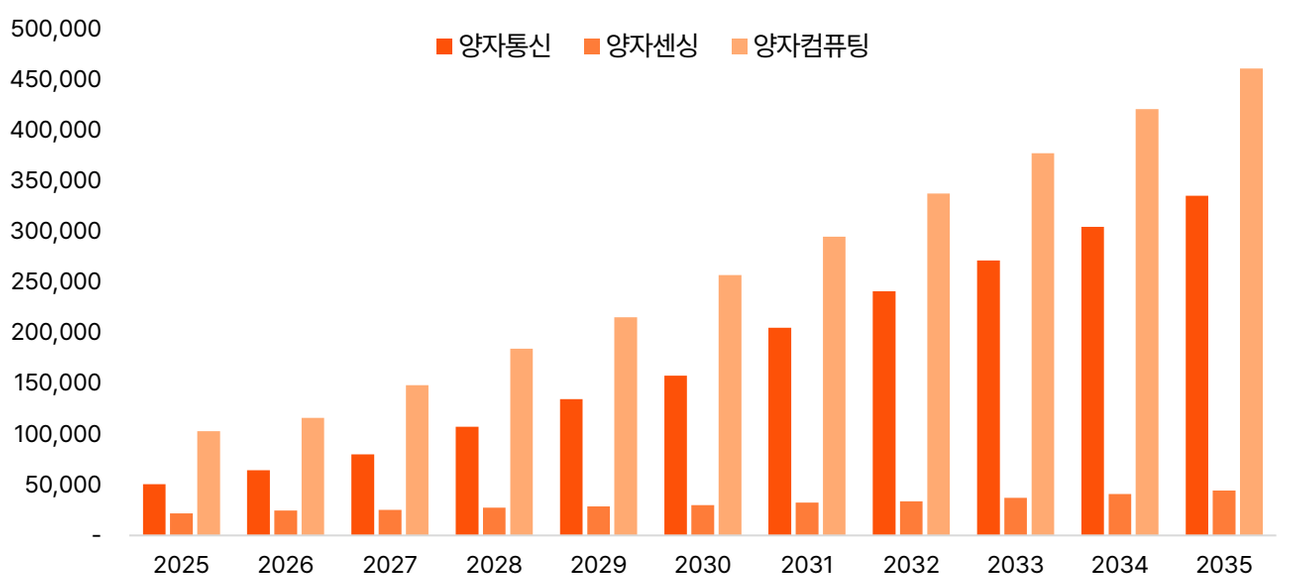
QKD 시스템이 효과적으로 작동하기 위해 필요한 요소가 양자난수생성기(Quantum Random Number Generator, QRNG)다. QRNG는 QKD 장비에 탑재되어 진정한 무작위 숫자를 실시간 만드는 역할을 수행한다. 기존의 난수생성기는 무작위 값을 도출하는 것처럼 보이지만 컴퓨터 알고리즘에 기반하고 있어 어쩔 수 없이 규칙성 · 주기성을 지니기 마련이다. 반면, QRNG는 빛의 양자인 광자의 편광 상태, 위상, 경로 등을 측정하여 패턴 분석이 아예 불가능한 무작위 값을 생성한다. 양자의 불확정성을 적용한 진정한 의미의 난수라 할 수 있다. 이 난수를 이용해 QKD 시스템은 양자 상태의 키를 보내고 측정한다.

3. 시장 전망 및 활용 분야

양자기술은 크게 양자컴퓨팅, 양자통신, 양자센싱의 세 축으로 구분된다. 잘 알려진 바와 같이 양자컴퓨팅은 큐비트를 통해 고전 컴퓨터 대비 연산 우위를 구현한다. 양자통신은 양자 상태 전송 및 물리 기반 보안을 제공한다. 마지막으로 양자센싱은 양자의 특성을 활용해 계측 기술의 정밀도 · 감도를 끌어올리는 영역이다.

글로벌 시장조사기관 Mind Commerce 등에 의하면 글로벌 양자기술 시장 규모는 2025년 약 17.5조원이며, 2035년까지 연평균 17%로 성장해 그 규모가 약 84조원에 이를 것으로 예상된다. 이 중 가장 비중이 큰 응용분야는 컴퓨팅으로 전체 시장의 50%를 상회하며, 양자통신은 2025년 29%에서 2035년 40%로 비중이 확대될 전망이다.

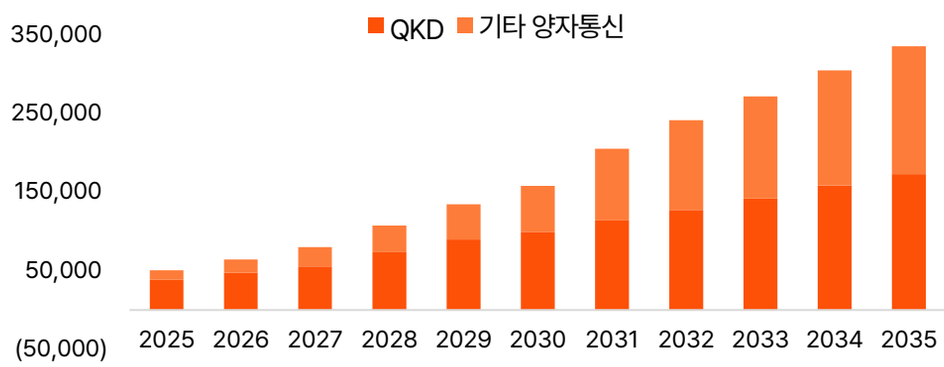
글로벌 양자기술 분야별 시장 전망 (단위: 억원)



자료: Mind Commerce(2025), 2025 양자정보기술 백서

양자통신 시장만 놓고 보면 2025년 규모가 5조원으로 추산되며, 연평균 21%씩 성장해 2035년 33조원을 돌파할 것으로 보인다. 본 보고서가 다루고 있는 양자보안 중 QKD가 바로 이 양자통신의 범주에 포함된다. QKD 시장은 2025년 3.8조원으로 양자통신 시장의 76%를 차지한다. 참고로 QKD와 함께 양자보안의 중요한 한 축을 담당하는 PQC는 복잡한 수학 계산을 활용하는 방식이므로 엄밀히 말해 양자통신이 아닌 고전 암호 분야에 해당한다.

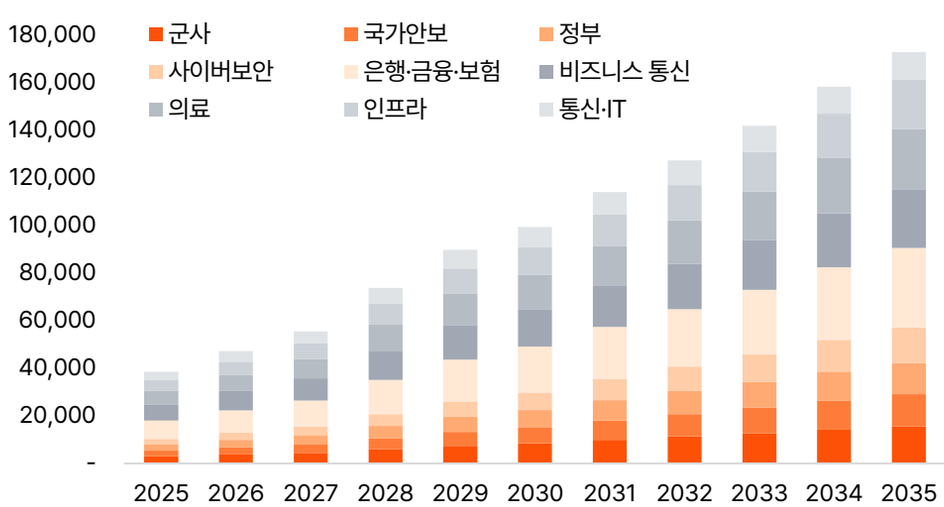
글로벌 양자통신 부문별 시장 전망 (단위: 억원)



자료: Mind Commerce(2025), 2025 양자정보기술 백서

이론적으로 완벽한 안전망을 구현하는 QKD는 보안 역량이 곧 경쟁력인 국방 · 공공 · 금융 · IT 등 다양한 분야를 망라하여 도입될 전망이다. Mind Commerce는 2035년 글로벌 QKD 시장 규모를 17조원으로, 수요산업별 비중은 금융업(19%), 의료(15%)가 높을 것으로 내다봤다. 금융업 등에 비해 시장 규모는 작지만 성장 속도로는 사이버 보안(연평균 20%), 국가안보(20%), 군사(18%) 영역이 상위권에 포진해 있다.

글로벌 QKD 수요산업별 시장 전망 (단위: 억원)



자료: Mind Commerce(2025), 2025 양자정보기술 백서

① 금융

금융 분야는 데이터 가치가 높고 HNDL 공격에 따른 피해 규모가 특히 크기 때문에 단기적으로 본사-지점 연결 등 주요 회선과 내부 핵심 시스템부터 양자보안 기술이 적용될 것으로 보인다. 금융 서비스에 쓰이는 인증서 · 서명 체계와 주요 전산 연결 구간의 보안 인프라를 보다 안전한 방식으로 교체하고, 중장기적으로는 결제 네트워크, 금융기관 간 정보 교환 등 더 넓은 영역으로 확대될 가능성이 높다.

2025년 5월 JP Morgan Chase는 광 섬유를 통해 두 개의 데이터센터를 연결하는 고속 양자보안 암호화 네트워크(Q-CAN)를 구축했다고 발표했다. 데이터센터를 연결하는 단일 광 섬유 및 QKD를 통해 독립적인 여러 가상 사설망(VPN)을 안전하게 보호할 수 있게 됐다. 양자기술 발전으로 해킹 우려가 커진 암호화폐 업계도 양자보안 도입에 적극적이다. 2026년 2월 국내 가상자산거래소 빗썸은 핀테크 보안기업 아톤과 기술협약을 체결하고 PQC 보안 솔루션을 플랫폼에 적용하기로 했다. 가상자산거래소에 요구되는 보안 수준이 높아진 데 따른 선제적 조치다.

② 제조

제조 분야에서는 스마트팩토리의 확산으로 제품 기획부터 완성까지 모든 생산과정이 정보기술로 통합되고, 현장의 실시간 제어가 중요해지고 있다. 그만큼 공정 간 데이터 교환, 생산 제어용 소프트웨어 등 내부망의 보안 침입이 큰 피해로 이어질 가능성도 커졌다. 단기에는 해킹 시 피해가 큰 중요 구간부터 통신망 보안을 강화하되, 단계적으로 라인 전체의 장치 모니터링 및 원격 설비 관리까지 양자보안을 표준화하는 변화가 예상된다.

③ 의료 · 제약

환자 데이터 · 임상 시험 결과 등 민감 정보가 많은 의료 · 제약 분야도 현재보다 강한 암호 구조가 요구될 여지가 크다. 병원-연구기관-클라우드 간 의료 데이터 전송 등 외부와의 연결 구간, 늘어나는 원격 진료 서비스, 신약개발 정보 교환에 양자보안 도입이 예상된다.

④ 교통 · 물류 · 항공

실시간 통신과 원격 제어가 중요한 교통 · 물류 · 항공 분야의 경우, 공항-관제센터, 물류 허브-운영센터 등 핵심 구간이 보안 구조 재편의 선순위다. 또한, 자율주행차 · 도심항공교통의 명령 및 실시간 상태 데이터 위 · 변조 방지가 전제되어야 이들 모빌리티를 활용한 운송 · 물류 혁신이 제대로 작동할 수 있다.

⑤ 국방 · 안보 · 우주

국방 · 안보 · 우주 분야를 보안 기술과 떼어 놓고 설명하기란 어불성설이다. 그만큼 양자보안 기술이 빠르게 도입 · 확산될 영역임을 쉽게 예상할 수 있다. 지휘 · 통제 상 군사통신 암호화가 필요하고, 군용 드론은 전장 데이터 위 · 변조로부터 안전해야 한다.

일례로 코스닥 상장사 사토시홀딩스(舊 딥파인드플랫폼)는 PQC 기반 드론 플랫폼 ARGUS-Q™을 출시하며 현대전의 Game Changer로 부상한 무인 전력시장을 공략하고 있다. 해당 플랫폼은 드론과 관제시스템 간 통신을 양자보안 알고리즘으로 암호화해 신호 교란 · 해킹 · 데이터 변조를 차단한다. 적의 전자전 공격 하에서도 드론이 수색 · 정찰 임무 수행을 작전대로 수행할 수 있게 된다.

사토시홀딩스의 PQC 드론 플랫폼 ARGUS-Q™

자료: 사토시홀딩스, 삼일PwC경영연구원

인류를 다시 달에 보내려는 아르테미스 프로젝트와 같이 우주경제가 본격 활성화되는 New Space 시대도 가시권에 들어왔다. 이에 위성과 지상국을 연결하는 통신망도 양자보안을 기본 인프라로 갖추게 될 확률이 높다.

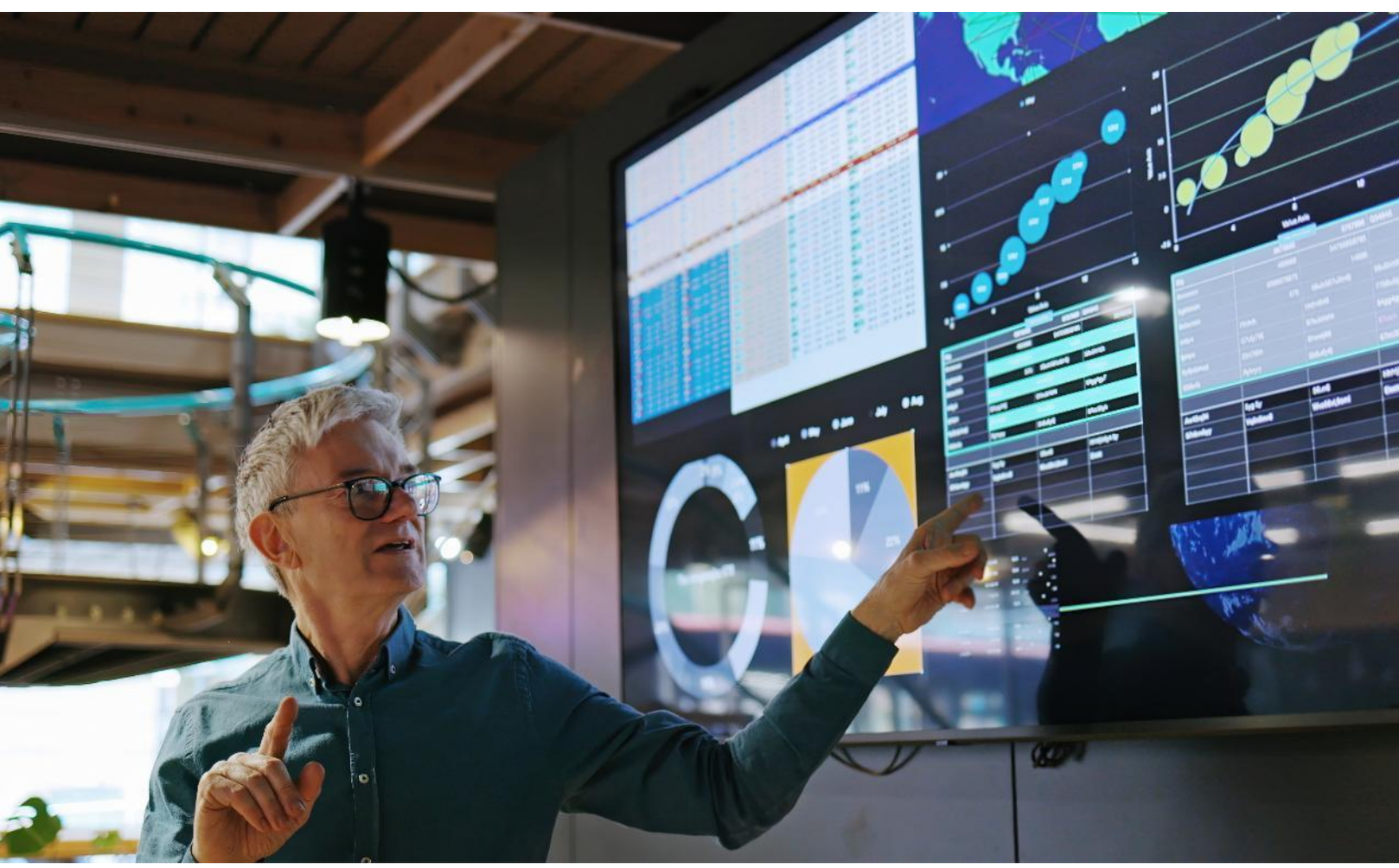
기존 알고리즘 하에서 위성 구간은 복잡성 및 처리 속도 지연 등의 문제로 암호화가 매우 어려운 영역이었다. 또한 국방 분야에서 사용하는 무선체계는 대역폭이 좁아 통신 속도가 저하되는 문제가 있었다. 이에 양자를 활용한 속도 및 성능 개선, 위성 구간 통신 암호화 등이 추진되고 있다.

⑥ 통신

통신은 양자보안이 특히 광범위하게 적용될 응용 분야다. PQC 기반 광 전송 장비, 네트워크 전반의 양자보안 탑재 등 인프라 수요부터 경량화 · 소형화된 암호화 시스템 보안 패키지, 양자인터넷 서비스 등 다양한 서비스가 창출될 전망이다. 독일 통신기업 Deutsche Telekom은 국내 보안 팹리스 아이씨티케이와 PQC 솔루션 프로젝트 협력을 진행하며 이동통신 산업에서의 디바이스 인증 및 네트워크 보안 강화를 추진했다.

III

양자보안,
누가 어떻게 만들고 있나



1. 국가별 동향

AI 활용 확대, 현대전의 변화 양상(무인 무기체계 · 정보 전쟁), 양자컴퓨터의 상용화 기대감 등 급변하는 시대 흐름 속에서 국가의 기술 주권은 보안에 달렸다고 해도 지나치지 않다. 이에 주요국들은 양자보안 개발에 박차를 가하며 수많은 창의 위협에 대비 중이다.

미국은 현재 PQC 표준화를 주도하며 PQC 도입을 권장하는 추세다. 기존 인프라 교체를 최소화하는 암호체계 업그레이드로 빠르게 자국 인프라를 보호하고, 글로벌 PQC 시장을 선점하는 전략이다. 미국 NIST의 PQC 표준 확정으로 RSA 등을 적용한 기존 암호체계는 폐기 수순을 밟고 있다. 기존 공개키 기반 인프라의 남은 수명은 길어야 2035년까지다. 반면, 미국 내 QKD 관련 동향은 PQC 대비 제한적이다. 이론적으로는 완전무결한 보안망이지만 당장 이를 구현하는 기술적 · 하드웨어적 한계로 인해 미국 국가안보국(NSA)이 QKD의 안전성에 회의적 입장을 취한 영향이다. 그러나 더욱 고도화된 양자컴퓨터 공격으로부터 완전히 자유로울 수 없는 PQC의 본질적 한계로 인해 중장기적으로는 미국도 결국 QKD를 주목할 것으로 판단된다.

중국은 광활한 국토를 양자암호통신으로 연결하기 위해 국가 프로젝트 차원에서 양자보안 개발에 뛰어들었다. 2016년 일찌감치 세계 최초의 양자통신 위성 묵자호를 발사해 장거리 지상국 간 양자통신에 성공했고, 베이징과 상하이를 잇는 세계 최장 수준의 양자암호 통신망도 구축했다. 2026년 장치 독립적 QKD(DI-QKD) 통신을 구현한 중국과학기술대의 연구 결과도 이목을 끌었다. DI-QKD는 장비의 신뢰도와 관계없이 통신 입출력 분석만으로 해킹 여부를 판단하며 기존 QKD보다 훨씬 어려운 기술로 꼽힌다. 하드웨어의 신뢰성 문제로 QKD 도입에 주저하는 미국과 상반되는 대목이다. 이로 인해 다수의 전문가들 사이에선 중국이 QKD를 비롯한 주요 양자통신 분야에서 미국을 앞서고 있다는 평가도 나온다.

중국의 양자통신 위성 묵자(Micius)호

자료: 중국과학원, 언론종합

유럽연합(EU)은 PQC와 QKD를 포괄하는 균형 잡힌 양자보안 전략을 추진 중이다. 2025년 EU는 양자컴퓨터 시대 사이버 위협에 대응하기 위한 양자보안 인프라 구축 전략을 공식 발표했다. 모든 주요 인프라에 대한 PQC 적용을 2030년까지 완료하고, 역내 금융 · 의료 · 통신 등 국가 핵심 데이터를 지키는 유럽 양자통신 인프라(EuroQCI)를 구축하는 내용이 골자다. 2026년에는 양자암호 위성 EAGLE-1을 발사하여 장거리 QKD 기술을 실증하고 각국 인프라 간 상호 운용성을 확보한다는 계획이다. 더불어 양자암호 적용 로드맵과 규제 체계를 담은 입법안 Quantum Act가 2026년 중 제정될 예정이다.

한국은 세계 최고 수준의 ICT · 통신 인프라에 공공 주도 시범사업을 더하며 PQC와 QKD를 동시에 정조준하고 있다. 과학기술정보통신부와 한국인터넷진흥원(KISA)은 2025년 에너지 · 의료 · 행정 등 주요 산업 대상으로 PQC 시범전환 사업을 추진했으며 2026년에는 시범전환 대상을 교통 · 국방 · 금융 · 우주 · 통신 등으로 대폭 늘렸다. 과학기술정보통신부는 2026년 1월 '제1차 양자과학기술 및 양자산업 육성 종합계획'을 발표, 공공 · 민간분야 전반의 PQC 전환과 전국 QKD망 확산 및 양자암호통신 상용화를 추진한다는 방침이다. 2028년까지 국가 핵심망 양자암호통신 구축, 2030년까지 위성 양자암호통신 개발이라는 단계별 목표도 제시했다. 통신 3사가 정부와 손잡고 전국 양자암호통신 구축 사업에 참여하고 있다. 한편, 2026년 지식재산처 발표에 따르면 한국은 2024년까지의 PQC 표준 대응 특허 출원량에서 미국을 제치고 세계 1위를 기록하며 PQC 기술 경쟁력을 입증했다.

양자보안 분야 주요국 현황 비교

기술력 우위

구분	미국	중국	EU	한국
PQC	2024년 NIST 표준화로 시장 선도, PQC 도입 가속화	PQC 행보 제한적, 미국 대비 열위	2030년 핵심 인프라 PQC 도입 목표	PQC 특허 세계 1위, 공공 주도 시범전환 추진
QKD	제한적 실증, 중국 대비 열위	위성 연계 등 대규모 실증, 세계 최대 QKD 통신망 구축, DI-QKD 등 고난도 기술 구현	2026년 양자암호 위성 연계 대규모 실증 계획	유선망 초기 실증, 2030년 위성 양자암호 통신 개발 목표

자료: 삼일PwC경영연구원

2. 해외 기업 사례

이제 주요 기업별 개발 동향을 살펴본다.

양자컴퓨터 개발을 선도하는 미국의 주요 기업 IBM, IonQ의 존재감은 양자보안에서도 드러난다. 2024년 미국 NIST가 발표한 세 가지 PQC 표준에는 IBM이 개발한 알고리즘이 2종(ML-KEM, ML-DSA)이나 포함됐다. 나머지 1종(SLH-DSA)도 IBM 연구진이 공동 개발한 것임을 감안하면 사실상 IBM이 글로벌 양자보안 기술의 이정표를 제시한 셈이다.

이온 포획 기반 양자컴퓨터를 개발하는 IonQ는 2025년 스위스 ID Quantique를 자회사로 편입했다. 양자보안 · 감지 시스템을 개발하는 ID Quantique의 특허 300여개 등 QKD, QRNG 기술 기반을 대량 확보하며 창과 방패를 모두 쥔 종합 양자 솔루션 기업으로 도약하고 있다. 같은 해 우주 광 통신기업 Skyloom 인수 계약도 체결, 지상과 우주를 잇는 양자보안 네트워크를 구축할 계획이다.

ID Quantique의 Clavis XG QKD 시스템

자료: ID Quantique

중국에서는 2025년 중국 국유기업 China Telecom의 자회사 China Telecom Quantum Group은 QKD와 PQC 기술을 결합한 양자 암호체계를 시연했다. 두 기술의 결합으로 보안성을 더욱 높였다는 평가다. 이 보안체계를 적용해 베이징과 안후이성 허페이까지 약 1,000km 구간의 양자암호 기반 통화에 성공했다고 발표했다.

양자보안 관련 해외 기업 동향

구분	주요 내용
IBM (미국)	• 2023년 양자보안 기술 이정표를 제시하며 IBM 퀀텀 세이프(Quantum Safe) 3단계 로드맵 발표 • 2024년 NIST PQC 표준으로 IBM이 개발한 ML-KEM(FIPS 203), ML-DSA(FIPS 204) 채택 • IBM 클라우드 및 다양한 자사 제품에 PQC 통합 진행
Google (미국)	• 양자컴퓨터 보안 위협에 대비해 크롬 브라우저 새 인증 체계 발표 • 기존 X.509 인증서에 용량이 큰 PQC를 직접 탑재하는 대신 데이터 크기를 최소화한 MTC(Merkle Tree Certificates)를 도입해 보안과 웹 브라우징 속도를 동시에 확보한다는 계획
QuSecure (미국)	• 기존 인프라를 전면 교체하지 않고, 보안 계층을 추가하는 방식으로 안전성을 확보하는 암호화 관리 플랫폼 QuProtect 제공 • 직관적인 인터페이스와 사용자 친화적 기능을 통해, 사용자가 PQC에 대한 전문 지식 없이도 암호화 관리와 보안 전환을 수행할 수 있도록 지원
IonQ (미국)	• 2025년 ID Quantique 인수를 통해 QKD, QRNG, 등 양자통신 기술을 확보하며 양자보안 솔루션 포트폴리오 구축 • 2025년 우주 광 통신기업 Skyloom 인수를 통해 지상과 우주를 연결하는 양자통신 인프라 확장, 장거리 · 글로벌 환경에서도 적용 가능한 차세대 양자 보안 네트워크 구축 목표 • 2026년 3월 루마니아 국가 양자통신 인프라 구축 완료(총 1,500km 이상 구간, 36개 양자보안 링크 포함)
ID Quantique (스위스)	• 양자기술 기반 보안 · 감지 시스템 개발 • 스위스 제네바에 양자보안 네트워크 구축 • 2018년 SK텔레콤이 인수 → 2025년 IonQ이 인수 • 2025년 QKD 장비 Clavis XG로 국가정보원 보안인증 획득
SEALSQ (스위스)	• NIST 표준 알고리즘을 사용하는 PQC 서비스 모듈, 양자 하드웨어에 보안 ASIC 설계를 통합한 보안 반도체 아키텍처 제공 계획
Thales (프랑스)	• 포스트 양자암호 연구 전담조직을 운영하며 독자적 양자내성 알고리즘 개발 • 2026년 5G SIM · eSIM에 PQC를 원격 적용하는 기술 공개 • 기사용 중인 카드나 단말을 교체하지 않고도 암호체계 전환 가능하여 인프라 교체 비용 절감 기대
Arqit Quantum (영국)	• 2025년 Intel, Equus Compute Solutions와 협력하여 양자보안 아키텍처를 모바일 통신에 적용
Toshiba Europe (일본/영국)	• 2025년 Deutsche Telekom의 광 섬유 네트워크를 통한 254km 장거리 QKD 통신 성공 • 양자시스템 유지를 위한 극저온 냉각 없이 상온에서 부품을 작동하여 상용화 가능성 입증
Huawei (중국)	• MWC 2026에서 네트워크 지능과 양자보안을 통합한 지능형 트래픽-암호 통합 솔루션 공개 • 별도의 양자암호 장비를 구축하지 않고도 기존 시스템에 양자보안을 직접 통합하여 아키텍처를 단순화하고 투자 비용 절감
China Telecom Quantum Group (중국)	• 1,000km 이상 떨어진 지역에서 PQC · QKD 결합 양자암호 기반 전화 통화 성공 • 통신사급 수준의 양자보안 메신저 플랫폼 Quantum Secret, 복잡한 행정 처리를 양자보안 환경에서 처리할 수 있는 Quantum Cloud Seal 등 기업용 서비스 확장

자료: 언론종합, 삼일PwC경영연구원

3. 국내 기업 사례

양자보안 분야에서 한국은 통신 3사 등을 중심으로 두각을 나타내고 있다.

SK텔레콤은 2024년 국내 양자 분야 핵심 기술 · 부품 기업들(에스오에스랩, 엑스게이트, 우리로, 케이씨에스, 노키아, IDQ코리아 등)과 함께 양자기술 얼라이언스 '엑스퀀텀'을 출범하고 양자암호 칩 Q-HSM을 공개했다. 2018년 인수한 스위스 양자통신 보안기업 ID Quantique 지분을 2025년 미국 IonQ에 넘기고 IonQ 지분을 확보하며 양자컴퓨터 역량도 확보 중이다. 전략적 제휴를 체결한 IonQ와는 공공 분야 양자암호 통신사업에서도 협업을 진행하고 있다.

KT는 통신망에 초당 30만개의 암호키를 생성 · 공급할 수 있는 QKD 장비를 개발했다. 1분에 7만대 이상의 암호 장비에 양자 암호키를 제공할 수 있으며, 필터 기술을 통해 광자 손실에 따른 오류율도 낮췄다. 스페인 바르셀로나에서 열린 세계 최대 정보통신 박람회 Mobile World Congress(MWC) 2026에서는 차세대 이동통신 6G 시대의 핵심 기술 중 하나로 '퀀텀 세이프 보안'을 제시하며 양자보안의 중요성을 거듭 강조했다.

SK텔레콤 주도 연합체 엑스퀀텀의 양자암호 칩 Q-HSM

자료: SK텔레콤

KT의 QKD 장비

자료: KT

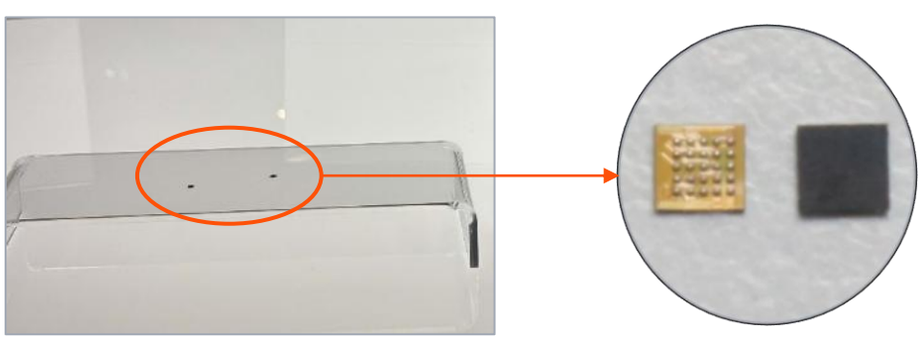
LG유플러스는 MWC 2026에서 AI 시대 사이버 위협에 대응하기 위한 차세대 보안 기술 4종을 선보였다. 이 중 PQC 광전송장비는 미국 NIST 및 국내 양자내성암호 연구단(KpqC)이 제시한 최신 PQC 알고리즘을 모두 지원하는 통합 인터페이스로 구현됐다. 2025년에는 ① PQC 장비(QENC)와 소프트웨어 정의 네트워크(SDN) 간 연동 인터페이스, ② SOLMAE 전자서명 방식을 한국정보통신기술협회(TTA)에 제안해 각각 국내 표준으로 제정되는 등 기술 표준화에도 적극 나서는 중이다. SDN 인터페이스 기술은 실시간 상태 모니터링, 인증서 관리, 정책 설정이 가능하며 이를 활용해 5G · 6G, 데이터센터, 국가 기간망 등 초고속 네트워크 환경에서 보안성을 강화할 수 있다. SOLMAE 전자서명은 메시지 무결성과 인증, 부인방지를 제공해 제3자가 메시지를 바꾸거나 속이는 것을 막는다.

LG유플러스의 PQC 지원 SDN 인터페이스

자료: LG유플러스

한편, 삼성전자는 업계 최초로 하드웨어 PQC를 탑재한 보안 칩 S3SSE2A을 공개, CES 2026 사이버보안 부문 최고혁신상을 수상하는 성과를 거두었다. NIST가 인증한 암호화 알고리즘을 활용해 칩 내부에서 안전한 데이터 처리 · 저장이 가능하다. 최근 출시한 갤럭시 S26에 탑재되는 애플리케이션 프로세서(AP) 엑시노스 2600에도 PQC 보안 기술이 적용됐다.

삼성전자 미국법인의 PQC 보안 칩 S3SSE2A



자료: 삼성전자, 삼일PwC경영연구원

양자보안 관련 국내 기업 동향

구분	주요 내용
SK텔레콤	• 2024년 국내 주요 양자기업들과 양자기술 동맹 엑스퀀텀 출범 및 양자암호칩 Q-HSM 공개 • 미국 IonQ와 전략적 제휴 체결하여 공공 분야 양자암호 통신사업 협업 진행 QRNG를 탑재한 스마트폰 갤럭시 퀀텀 출시
KT	• 초당 30만개의 암호키를 생성할 수 있는 QKD 장비 개발 • 개방형 양자 테스트베드 구축 · 운영 사업에 참여, 양자암호통신 통합 관제 플랫폼 시범 운영 • 2025년 자체 개발 QKD 기술이 적용된 장비로 국가정보원 보안검증 통과
LG유플러스	• MWC 2026에서 PQC 광전송장비 포함 차세대 보안 기술 4종 공개 • PQC 지원 SDN 인터페이스와 SOLMAE 전자서명 방식 제안 및 국내 표준으로 제정
삼성전자	• 갤럭시 S26에 탑재되는 모바일 애플리케이션 프로세서(AP) 엑시노스(Exynos)에 PQC 기반 보안 기술 적용 • 미국 NIST가 선정한 표준 양자 내성 암호 알고리즘 ML-DSA 채택 PQC 보안 칩 S3SSE2A으로 CES 2026 사이버보안 부문 최고혁신상 수상
사토시홀딩스	• 드론과 관제시스템 간 통신을 양자보안 알고리즘으로 암호화해 해킹·데이터 변조를 차단하는 PQC 기반 드론 플랫폼 ARGUS-Q 공개 • 전쟁 · 재난 등 위험 환경에서 드론 기반 수색·정찰 임무 수행에 적합하도록 설계
엑스게이트	• QRNG를 적용해 예측이나 복제가 사실상 불가능한 고품질 난수를 지속적으로 생성하는 VPN 솔루션 Quantum VPN 제공
코위버	• 2024년 1G/10G/100G급 양자통신암호장비의 국가공인기관 인증 획득 • 퀀텀플럭스와 함께 저비용, 소형화 QKD 송수신기 모듈 개발 과제 수행
시큐센	• 보안기술연구소에서 암호 기반 라이브러리를 개발해 한국인터넷진흥원(KISA)의 국내 암호모듈검증제도(KCMVP) 인증 획득 • 2025년 양자내성 기반 상호인증 및 구간암호 솔루션 아이인젝션(iEnxection) PQC 출시
라온시큐어	• 전자서명과 구간암호화 기능을 PC 환경에서 제공하는 Key#Biz, 모바일 환경에서 제공하는 Key#Wireless에 PQC 기술 적용 • 2025년 PQC를 적용한 모바일 가상 키패드 솔루션 터치엔 엠트랜스키(TouchEn mTranskey) v5.0으로 한국정보통신기술협회(TTA) GS인증 1등급 획득
우리넷	• KCMVP 인증 모듈이 적용된 양자통신 암호화 장비 개발 및 보안기능확인서 획득 • SK브로드밴드와 공동 개발한 패킷 기반 하이브리드 키 방식 암호화 전송장비를 한국전력기술 통신망에 적용

자료: 언론종합, 삼일PwC경영연구원

IV

시사점 및 제언

1. 시사점

창보다 방패가 먼저 필요하다.

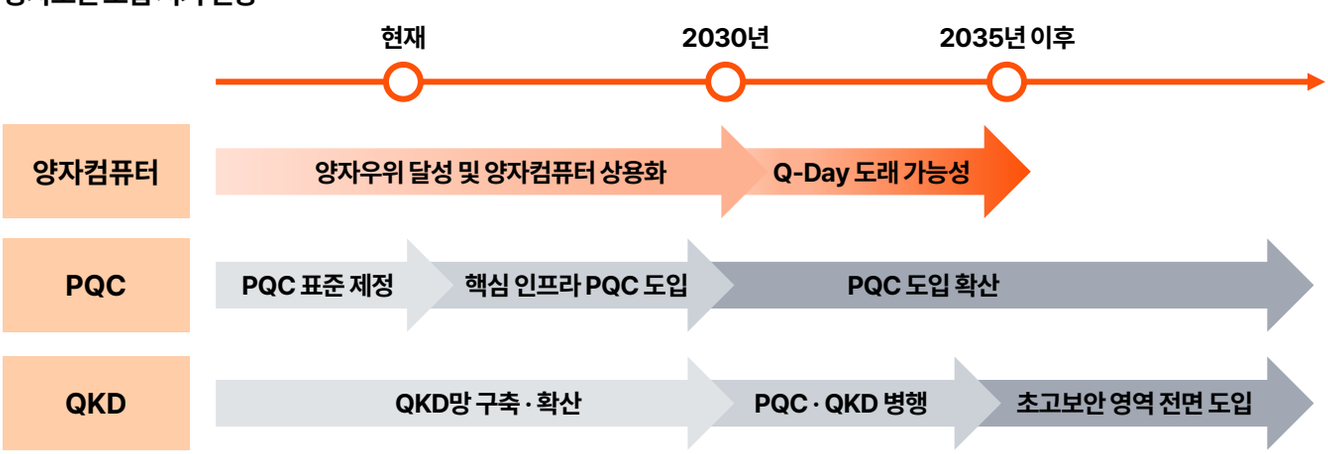
양자컴퓨터 기술은 나날이 발전하고 있지만 완전한 상용화 시점보다 양자보안 시장이 먼저 개화할 것이 확실하다. 아직 양자컴퓨터 상용화까지는 충분한 큐비트 수 확보 및 안정성 유지, 오류정정 등 넘어야 할 기술적 난제들이 남아 있다. 하지만 AI의 활용 범주 · 정보 접근 권한이 확대되고, 드론을 위시한 무인무기체계가 현대전의 핵심 역량이 되었으며, HNDL 위협도 현실화되는 가운데 정부와 산업계는 당장 보안체계 전환 압박에 직면할 수밖에 없다. 세계 각국과 주요 기업들이 양자보안 기술 표준 수립 · 개발에 사활을 걸고 있는 만큼 양자컴퓨터가 현재의 디지털 보안을 무력화하는 이른바 Q-Day의 우려는 머지않아 불식될 것으로 보인다.

대세는 PQC, 초고보안 영역은 QKD

양자내성암호(PQC)는 기존 인프라에 올릴 수 있는 소프트웨어 업그레이드에 가깝고, 양자키분배(QKD)는 하드웨어의 근본적 변화를 수반하는 보안 혁신으로 아직까지 비용과 전송 거리의 물리적 제약 등이 존재한다. 두 기술은 대체재 관계에 있기보다는 서로 다른 계층적 보안체계를 구현하는 보완적 관계에 가깝다.

PQC는 기존 네트워크 · 장비와의 호환성이 높고 빠른 전환이 가능해 경제성과 확장성 측면에서 유리하다. 한편, '현재의' 양자컴퓨터가 풀기 어려운 수학적 난제가 '앞으로 나올' 양자컴퓨터 앞에서도 제 기능을 할지는 미지수인 만큼 국가 기간망, 중앙은행, 전력 제어망 등 보안 사고의 여파가 막대한 영역에서는 이론상 완벽한 보안을 구현하는 QKD가 종착지가 될 것으로 보인다. 당장은 PQC가 상용화 및 확산을 주도하고 있고, QKD 인프라 구축의 복잡성, 시스템 교체 비용, 장비의 신뢰성 문제 등이 발목을 잡지만 그럼에도 QKD의 길을 포기해서는 안 되는 이유다.

양자보안 도입 시기 전망



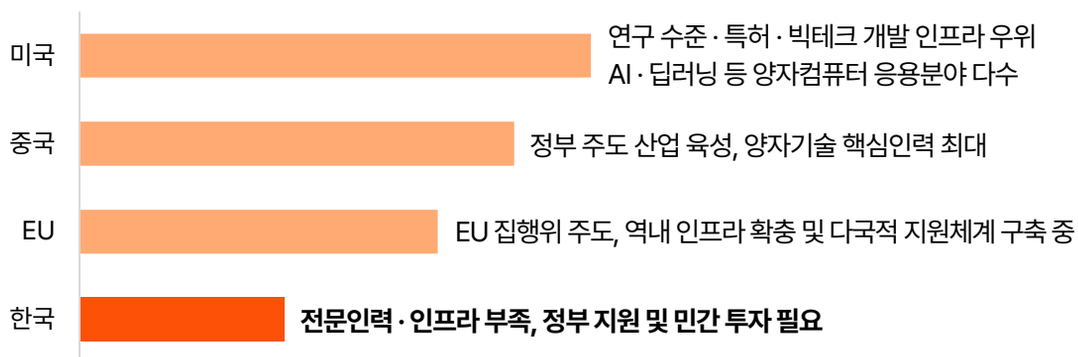
자료: 삼일PwC경영연구원

한국에게는 양자보안이 기회의 장

한국의 양자컴퓨터 기술 역량은 해외 주요국과의 격차가 여전히 큰 상황이다. 한때 정부가 국산 기술로 2032년까지 달성하겠다고 계획했던 1000큐비트 양자컴퓨터는 미국 IBM이 2023년 공개한 Condor(1,121큐비트)와 엇비슷한 수준이다. 단순 계산으로 보더라도 글로벌 선도기업과는 9년의 기술 격차가 존재한다. IBM이 Condor를 선보일 당시 국내 양자컴퓨터는 20큐비트 수준에 불과했다. 이렇듯 양자컴퓨터 자체 개발의 진입장벽이 높은 만큼 국내에서는 외부 양자컴퓨터를 활용해 신소재를 개발하는 등 응용사례를 만드는 데 집중하고 있다는 분석도 나온다.

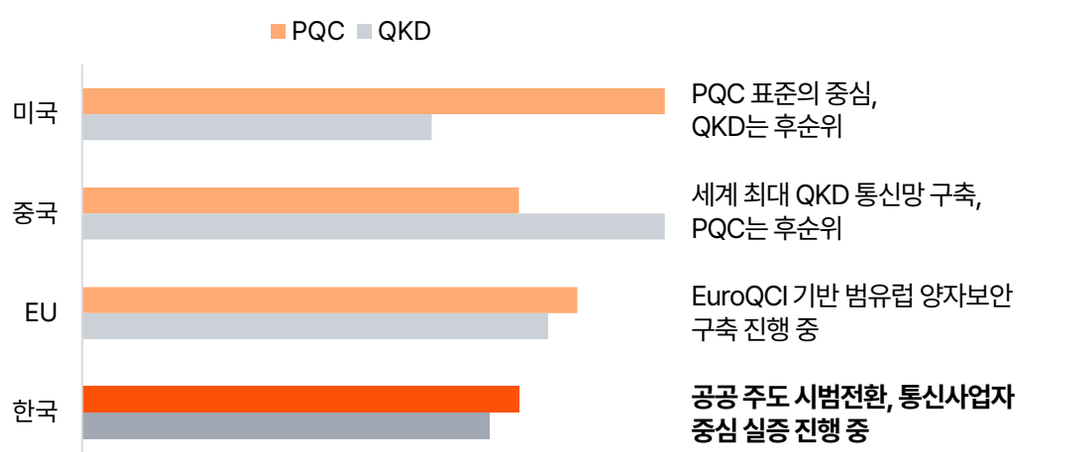
반면, 양자보안 영역에 있어서는 상대적으로 격차가 적고 PQC 관련 특허 출원 수에서 확인되듯 일부 분야에서는 충분한 경쟁력이 있는 것으로 나타난다. 여전히 해외 기업들이 기술을 선도 중이지만 한국은 세계 최고 수준의 ICT · 통신 인프라 보유국으로 양자보안 기술의 상용화 · 확산 측면에서 유리한 조건을 갖추고 있다. 양자보안 기술 지형은 양자컴퓨터처럼 하드웨어 중심 고난도 경쟁만 있는 것이 아니므로 통신 인프라 · 암호 알고리즘 전환 · 국제표준 등 실증 · 응용 영역에서 충분히 승부를 걸어볼 수 있다.

주요국 양자컴퓨터 경쟁력 비교



자료: 삼일PwC경영연구원

주요국 양자보안 경쟁력 비교



자료: 삼일PwC경영연구원

2. 제언

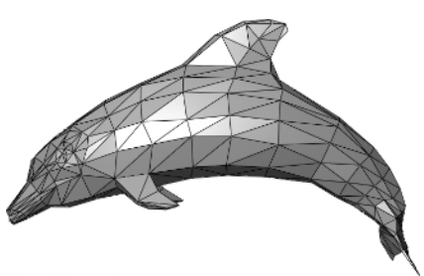
국제 표준 제정 참여의 중요성: NVIDIA도 처음엔 망할 뻔했다

양자보안 시장은 현재 초기 단계에 있고 그 잠재 규모가 더욱 커질 것이 확실시되는 만큼 기술 리더십과 시장 주도권 확보 노력이 필요하다. 이러한 노력의 일환으로 국제 표준화 무대에서 한국의 영향력이 더욱 강화돼야 한다. 표준과 인증을 확보하는 국가가 글로벌 시장 선점효과와 공급망 우위를 가져갈 것임은 자명하다. 미국 NIST가 PQC 표준 제정을 주도 중이고, QKD 역시 유럽전기통신표준화기구(European Telecommunication Standard Institute, ESTI), 국제전기통신연합(International Telecommunication Union, ITU) 등을 중심으로 표준 경쟁이 벌어지고 있다. 시장 개화를 앞둔 현 시점, PQC 알고리즘의 상용화 · 적용 가이드라인, QKD 네트워크 관리 표준 등은 향후 산업의 전체 구조를 좌우할 가능성이 크다. 창업 초기 제품 표준 문제로 벼랑 끝에 몰렸던 NVIDIA의 사례를 반면교사하여 정부와 유관기관, 기업 모두 표준 활동에 참여해야 한다.

※ NVIDIA 초기 사례

초창기 기술 표준의 중요성을 알 수 있는 에피소드로 NVIDIA 사례를 소개한다. 현재 글로벌 반도체 팹리스 1위인 NVIDIA가 처음부터 잘 나갔던 건 아니다. NVIDIA 설립 초기, 그래픽 카드 시장에서는 특정 다각형을 여러 개 붙이는 방식으로 3D 그래픽을 구현했는데, 어떤 도형을 기본으로 할지에 대한 표준은 부재했다. 문제는 NVIDIA가 사각형 기반 제품 개발에 몰두한 반면, 동종업계에서는 점차 삼각형이 대세로 자리잡기 시작했다는 점이다. 여기에 뒤늦게 Microsoft가 삼각형 기반 3D 그래픽 표준 API를 내놓은 게 결정타가 됐다. 졸지에 업계 표준에 부합하지 않는 외로운 길을 가게 된 NVIDIA는 제품 개발이 중단되는 등 실패를 거듭하며 자금난에 몰렸다가 1997년 RIVA 128 NV3의 성공으로 가까스로 기사회생한다. 이후 1999년 최초의 GeForce 제품을 출시하며 본격적으로 GPU 시장을 개척, 오늘날의 반도체 제국을 이뤄냈다.

삼각형 기반 3D 그래픽 예시



자료: Wikipedia

기존 암호체계 · PQC 결합 하이브리드 전략: 속도와 안정성 두 마리 토끼를 잡자

양자보안 도입은 속도전이다. 하지만 PQC가 기존 인프라와 호환성이 높다 해서 하루 아침에 도입할 수 있는 건 아니다. 기존 시스템 · 네트워크 · 디바이스 등이 전환 과정에서 성능 저하나 운영 중단이 발생할 여지는 없는지 다각도로 검증이 필요하다. 기존 암호체계와 PQC 도입을 병행하면서 PQC 적용 범위를 단계적으로 확장하는 하이브리드 전략이 속도와 안정성 모두를 잡는 방안이다. 언론 보도에 따르면, TLS 통신(인터넷에서 브라우저와 서버 간 데이터를 암호화하는 보안 프로토콜)에서 기존의 타원곡선암호와 격자 방식 PQC를 결합해 키를 생성하는 방식의 효과성이 Cloudflare와 Google의 실험을 통해 입증된 바 있다. 전자서명에서도 현재의 RSA와 격자 PQC를 동시 적용한 다중 서명구조를 고안할 수 있다. 또한 진정한 난수를 생성하는 QRNG를 기존 암호 알고리즘에 적용하는 것도 보안성을 높이는 유효한 접근이다.

소재 · 부품 · 장비 육성: 함께 가야 더 멀리 간다

글로벌 양자보안 시장을 주도할 대표 기업 육성은 당연히 중요한 과제다. 더불어 이를 뒷받침할 산업 생태계 조성이 절실하다. 양자보안은 단일 산업이 아니다. 칩 · 광학 모듈 · 소프트웨어 · 보안 장비 등이 복합적으로 맞물려 가치를 창출한다. 즉, 소부장 기반이 탄탄해야 대표 기업이 나올 수 있고 진정한 의미의 기술 강국으로 부상할 수 있다. 삼성전자 · SK하이닉스 같은 메모리 기업과 한미반도체 · 주성엔지니어링 등 소부장 기업들이 함께 산업 경쟁력을 끌어올린 반도체만 보더라도 알 수 있는 사실이다.

2026년 1월 정부는 '제1차 양자과학기술 및 양자산업 육성 종합계획'에서 지역과 산업을 잇는 양자 클러스터를 조성하고, 산학연 역량을 결집하여 산업 기반을 구축한다는 기본방향을 제시했다. 소부장 핵심 품목을 도출하여 국내기업을 전략적으로 육성하는 방안도 담겼다. 이 같은 지원계획이 실질적으로 소부장 국산화를 앞당기고 양자보안 Value Chain 확장을 가속화하는 장기적 우위를 가져오길 기대한다.

[Appendix 1]

양자역학 및 양자컴퓨터의 기본 개념

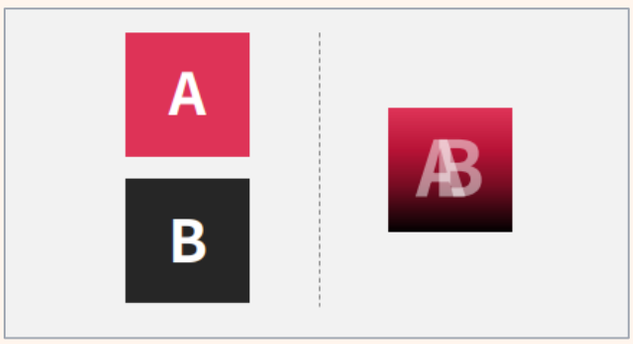
양자보안 주제를 다룬 본 보고서는 양자컴퓨터에 대한 기초적인 이해를 전제로 작성되었다. 이에 본 부록에서는 양자컴퓨터의 작동 원리와 그 근간이 되는 양자역학의 기본 개념을 간략히 설명한다.

양자컴퓨터를 설명하기 위해서는 양자역학을 먼저 짚고 넘어가야 한다. 양자(Quantum)란 아주 작은 물질이나 에너지 단위를 의미하며, 물질을 구성하는 원자, 빛의 기본 단위인 광자 등이 여기에 포함된다. 이렇게 미세한 양자의 세계에서는 우리가 일상에서 접할 수 없는 물리법칙이 작용하며, 이를 설명하는 이론이 양자역학이다.

이 중 양자컴퓨터를 이해하기 위해 알아야 할 두 가지 개념만 대표적으로 설명한다. 먼저 양자중첩(Quantum Superposition)이다. 이는 여러 가능성이 겹쳐 있는 조합을 뜻한다. 중첩 상태에 있는 전자는 특정 지점에 명확히 자리잡고 있는 게 아니라 여러 곳에 있을 확률이 겹쳐진 상태로 존재한다. A일수도 B일수도 있는 가능성이 한데 겹쳐 있는 상태에서 우리가 관측을 하는 순간에야 비로소 A와 B 중 한 가지 상태로 결정된다는 특성이다.

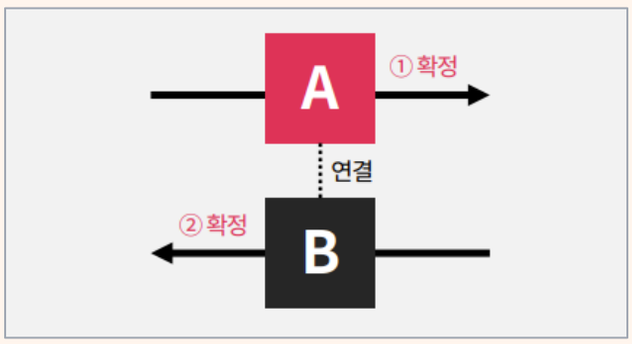
양자역학이 다루는 또다른 특성으로 양자얽힘(Quantum Entanglement)이 있다. 이는 두 개 이상의 양자가 한 몸처럼 연결되어 행동하는 현상으로, 두 입자가 아무리 멀리 떨어져 있어도 서로의 상태에 영향을 주는 상관관계를 뜻한다. 예를 들어 두 입자가 스핀이라는 양자 상태로 얽혀 있다면, 한 입자의 스핀 방향을 측정하는 순간 다른 한 입자의 스핀도 즉시 결정되며, 두 측정 결과는 밀접한 관계를 갖는다.

양자중첩



자료: 삼일PwC경영연구원

양자얽힘



자료: 삼일PwC경영연구원

이러한 양자역학의 기본 개념들은 우리의 상식으로는 이해하기 어렵지만 수많은 실험들을 통해 그 현실성이 입증되었으며 이를 토대로 오늘날 양자컴퓨터가 개발되고 있다.

현재의 컴퓨터는 0과 1 중 한 가지 값을 갖는 비트(Bit)를 통해 연산을 수행한다. 반면, 양자컴퓨터는 양자역학의 성질을 적용한 큐비트(Quantum Bit, Qubit)를 연산단위로 사용한다.

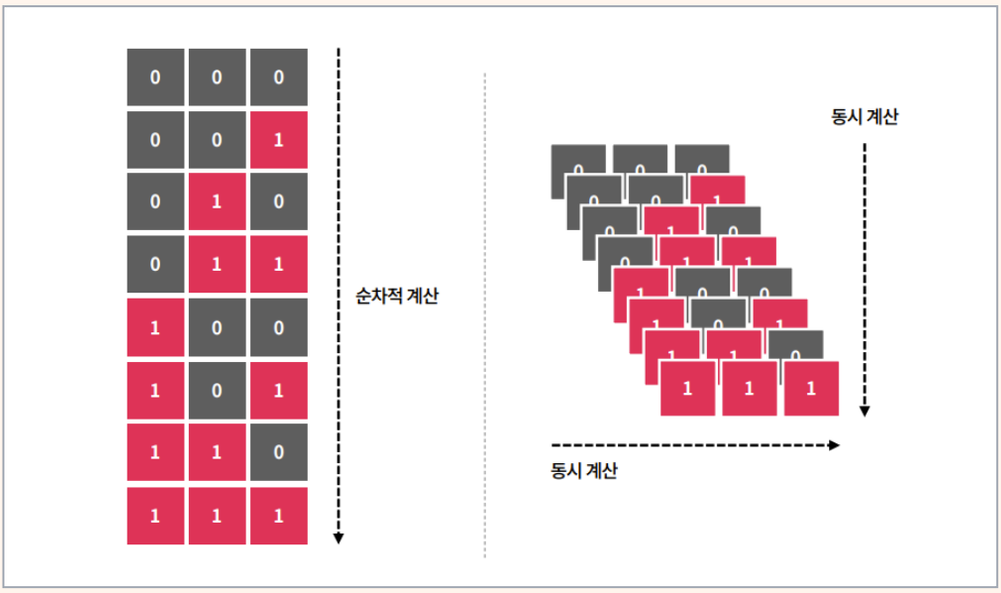
큐비트는 0과 1이 중첩된 상태로 동시에 존재할 수 있으며, 여러 큐비트끼리 서로 얽힘으로 연결될 수도 있다. 그 결과, 양자컴퓨터는 단순한 0과 1 조합 이상의 막대한 양의 정보를 한꺼번에 처리할 수 있게 되며 기하급수적인 계산 속도 향상을 이끌어낸다. 하드웨어의 업그레이드 수준을 넘어서는 컴퓨팅 기술의 근본적인 패러다임 변화라 할 수 있다.

기존 컴퓨터와 양자컴퓨터의 기본 개념 비교

구분	기존 컴퓨터	양자컴퓨터
작동 원리	CPU 내부 트랜지스터를 이용하여 전기 신호(0과 1) 제어	전자의 이중성 등 양자역학 원리를 정보처리에 적용
기본 단위	비트	큐비트
비트 n개의 정보량 표현	2^n개 중 한 번에 1가지 결과값만 표현	2^n개 전체 결과값을 동시에 표현
연산 방법	논리 표에 의한 반복 계산 (직렬계산)	행렬 함수에 의한 동시 계산 (병렬계산)

자료: 삼일PwC경영연구원

기존 컴퓨터(좌)와 양자컴퓨터(우)의 연산 개념 비교

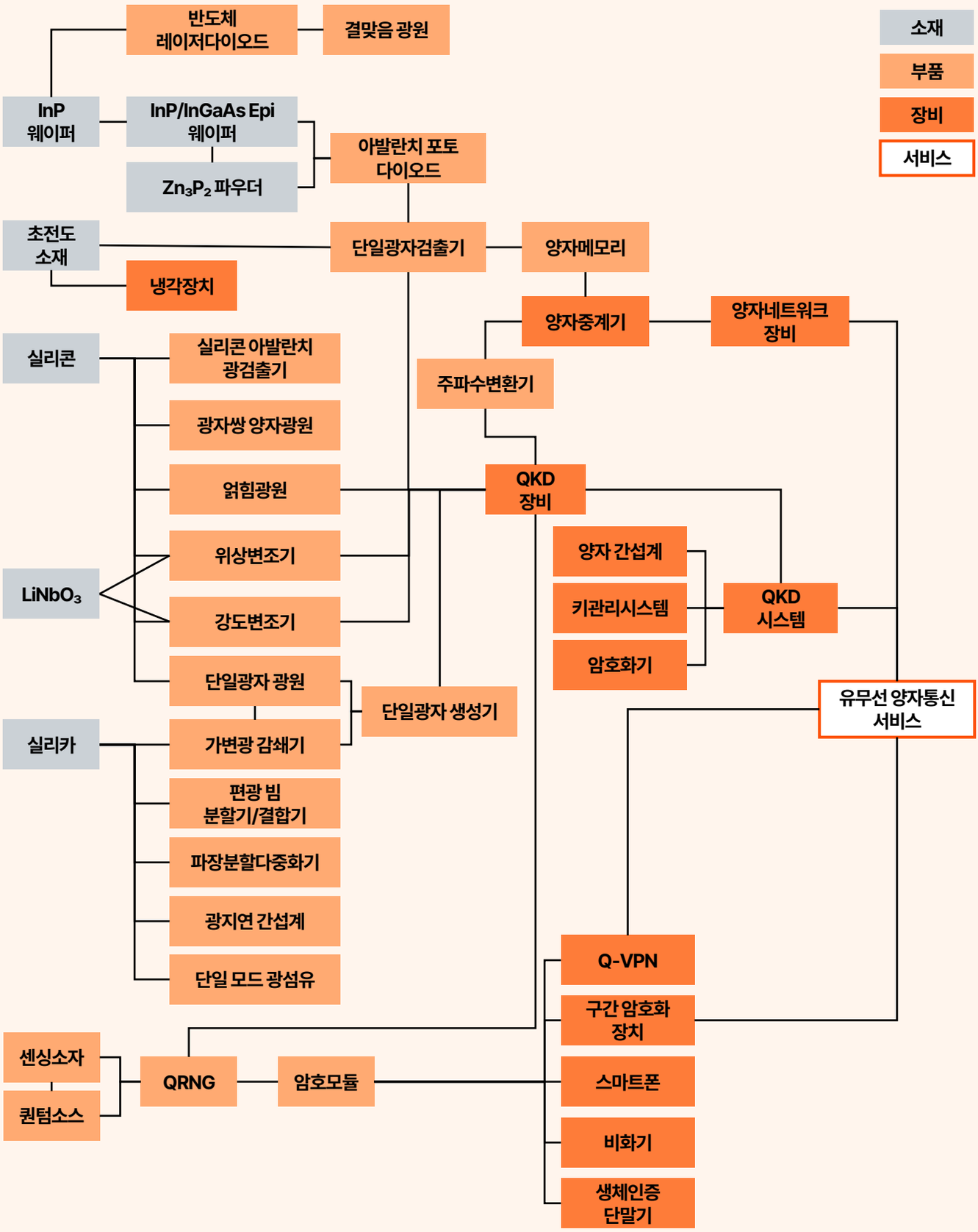


자료: 삼일PwC경영연구원

양자컴퓨터 개념 및 활용 사례는 「큐비트의 마법, 상상을 계산하는 양자컴퓨터 혁명(2025.03)」 참조

[Appendix 2]

양자통신 Value Chain



자료: 양자산업생태계지원센터, 삼일PwC경영연구원

[Appendix 3]

양자통신 소재 · 부품 · 장비 목록

분류		제품명	주요 공급처
소재	양자키분배	인듐인(InP) 웨이퍼	Vital Materials, Acrotec, Wafertech, InPACT, Wafer World Inc., Powerway Wafer, Biotain Crystal, PAM-XIAMEN, Biotain crystal, 웨이퍼비즈, MTI Korea
		에피택셜 웨이퍼	IQE, Coherent, LandMark, Intelliepi, QSI, 에피솔루션, 한국광기술원, 한국나노기술원
		인화아연(Zn_3P_2) 파우더	티파인, 하나로티알, Funcmater
		실리카(SiO_2)	한국첨단소재, GAOTek, Montclair Fiber Optics, Optcore, Neon Photonics, 우리로
		실리콘(Si)	AMF, AIM Photonics, Tower Semiconductor, SMART Photonics, CEA-LETI Photonics, IHP, imec, LioniX
		리튬나이오베이트 ($LiNbO_3$)	NanoLN, MSE Supplies
		단일광자 검출기용 소재(NbN, NbTiN, WSi, MoSi 등)	Photon Spot, Single Quantum, Scontel, Quantum Opus, PIXEL Photonics, PHOTEC, ID Quantique, Hamamatsu, Micro Photon Devices, Quantum Machines
부품	양자키분배	단일 모드 광섬유	LS전선, 대한광통신, 가온전선, 세종전선, 한국미래소재
		레이저 다이오드	QPHOTONICS, OPTILAB, FITEL, Thorlabs
		아발란치 포토 다이오드	우리로, ID Quantique, Micro Photon Devices
		위상변조기	iXblue, EOSpace, PSI, JenOptik
		강도변조기	iXblue, EOSpace, JenOptik, Thorlabs, Conquer Photonics
		가변광감쇄기	AC Photonics, Lumentum, Keysight, OZ Optics, JDSU(VIAVI), Santec
	양자난수생성기 기반 제품	양자난수생성기(QRNG)	이와이엘, ID Quantique, Quintessence Labs, Quside, QuantumCTek
		암호모듈	이와이엘, 케이씨에스
장비	양자키분배	양자키분배 장치(QKD)	코위버, 우리넷, 에프아이시스, IDQ, 도시바, SK텔레콤, QuantumCTek
		양자키관리시스템(KMS)	다임즈, 드림시큐리티, ID Quantique
	양자난수생성기 기반 제품	양자 가상사설망 (Q-VPN)	안랩, XN시스템즈, 시큐어넷시스템즈, 퓨쳐시스템
		스마트폰	삼성전자
		비화 단말기	에이스안테나, 쎄트렉아이, LIG넥스원
		구간 암호화 장치	이와이엘
		생체인증 솔루션	옥타코
		지문인식 제품	옥타코

자료: 2024 · 2025 양자정보기술 백서

Business Contacts

이 승 환 Partner
seung-whan.lee@pwc.com

박 현 출 Partner
hyunchul.park@pwc.com

김 태 형 Partner
taehyung2.kim@pwc.com

이 성 호 Partner
sungho1.lee@pwc.com

정 성 문 Partner
sungmoon.cheong@pwc.com

Author Contacts

삼일PwC 경영연구원

이은영 상무
eunyoung.lee@pwc.com

안정효 선임연구원
jeonghyo.ahn@pwc.com

삼일PwC 경영연구원

최재영 경영연구원장
jaeyoung.j.choi@pwc.com

S/N: 2604W-RP-050

pwc.com/kr