한눈에 보는 한국형 양자내성암호(KpqC)와 지식재산(IP) 트렌드

양자 위협에 맞서는 대한민국의 해답,
KpqC와 IP, 보안을 넘어 기술 주권으로,
대한민국 IP의 새로운 미래를 엽니다.

지식재산처 양자내성암호연구단 한국특허기술진흥원

위협의 본질 : Harvest Now, Decrypt Later

양자 컴퓨터가 상용화된 후에는 돌이킬 수 없습니다. 지금부터 준비해야 합니다.

현재(Present)	시간 경과	미래(Future)
암호화된 데이터 탈취 및 저장	**데이터 보관 (Data Storage)**	**양자 컴퓨터 등장 및 암호 해독**
현재 기술로는 해독 불가능하지만 무차별 수집		과거의 모든 비밀이 일시에 노출

기존 암호의 붕괴

소인수분해 및 이산대수 문제에 의존하는 RSA, ECC 등의 현대 암호체계는
양자컴퓨터의 쇼어 알고리즘(Shor's Algorithm)에 의해 순식간에 무력화됩니다.

HNDL 공격의 실체

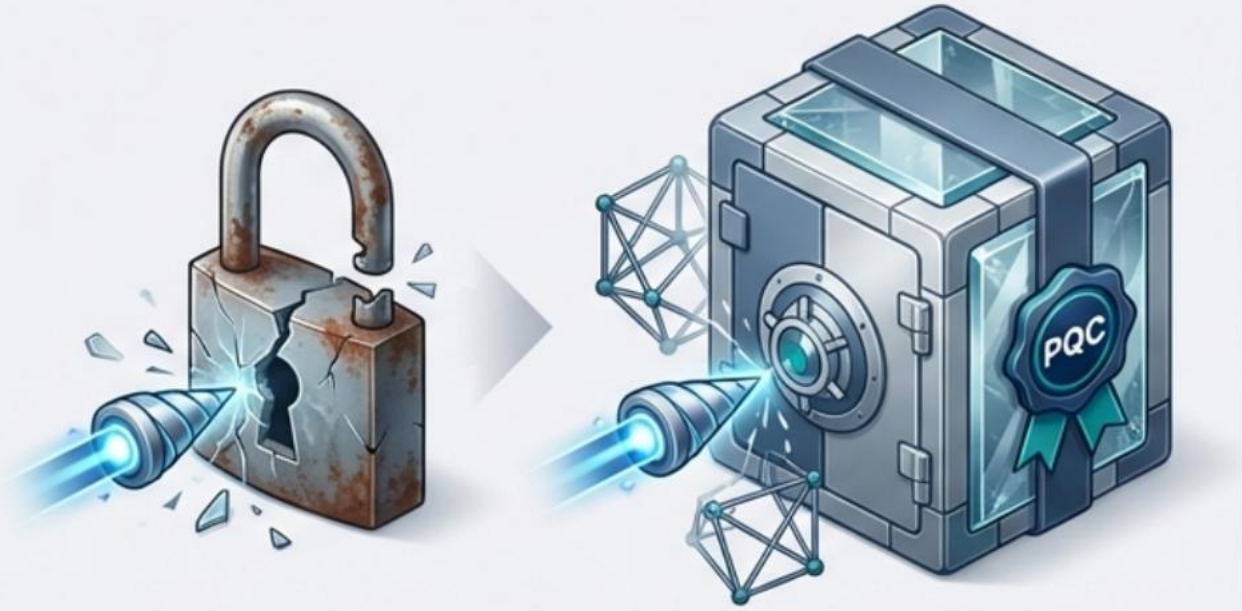
해커들은 지금 당장 해독할 수 없더라도 암호화된 데이터를 수집하고 있습니다.
미래에 양자컴퓨터가 등장하는 순간, 과거의 모든 비밀을 해독할 수 있습니다.

PQC: 양자컴퓨터로도 뚫을 수 없는 금고

PQC란?

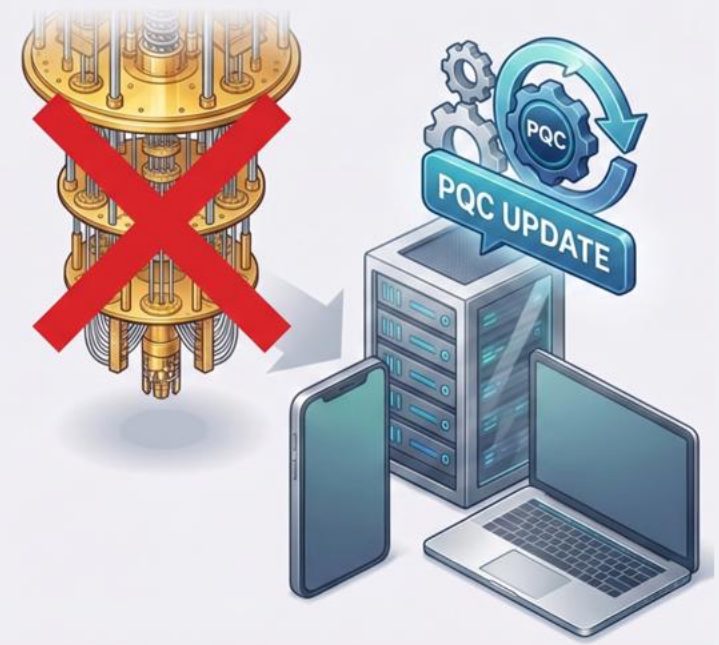
양자내성암호(PQC)란 양자 컴퓨터라는 '초강력 드릴'도 뚫지 못하도록, 새로운 방식의 수학적 재질로 설계된 암호 체계입니다.

* **(양자내성암호)** 양자컴퓨터로도 해독하기 어려운 수학적 문제를 기반으로 하는 암호 기술로, 양자컴퓨터 시대에도 안전하다는 뜻에서 포스트-양자암호(Post-Quantum Cryptography, PQC)로 지칭



핵심 장점

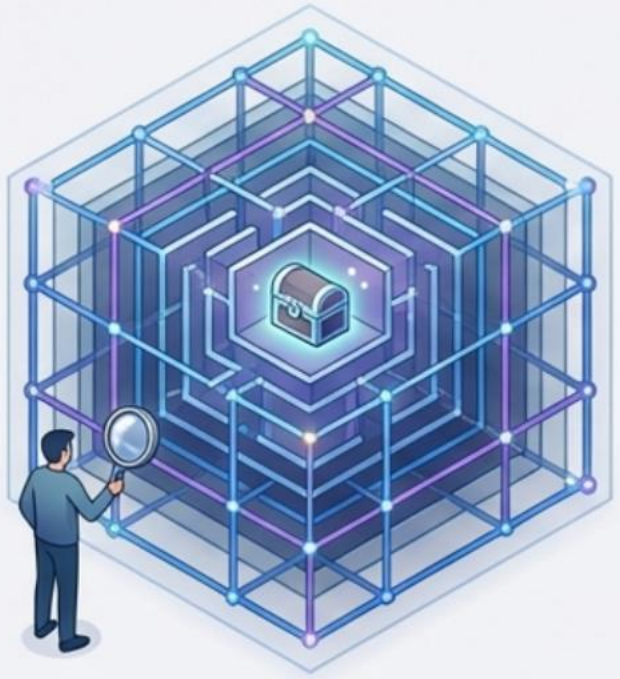
별도의 고가 양자 장비가 필요하지 않습니다.
현재 우리가 사용하는 PC, 스마트폰 등 기존 IT 인프라 위에서 암호 소프트웨어 등 업데이트만으로 구현 가능합니다.



쉽게 이해하는 PQC의 3가지 핵심 원리

1. 격자 기반(Lattice)

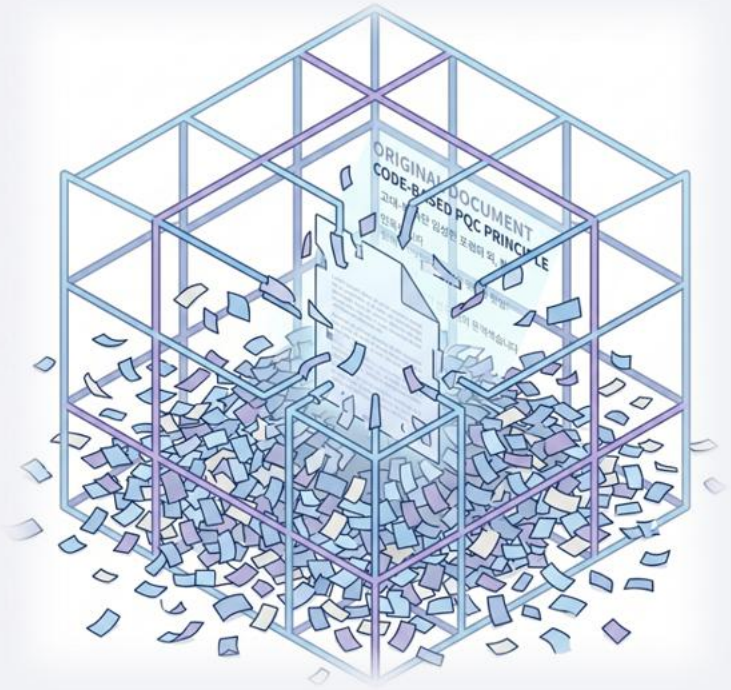
초고차원 미로 속 보물 찾기



수조 개의 점으로 구성된 고차원 공간에서 숨겨진 한 점을 찾는 난제입니다.

2. 코드 기반(Code)

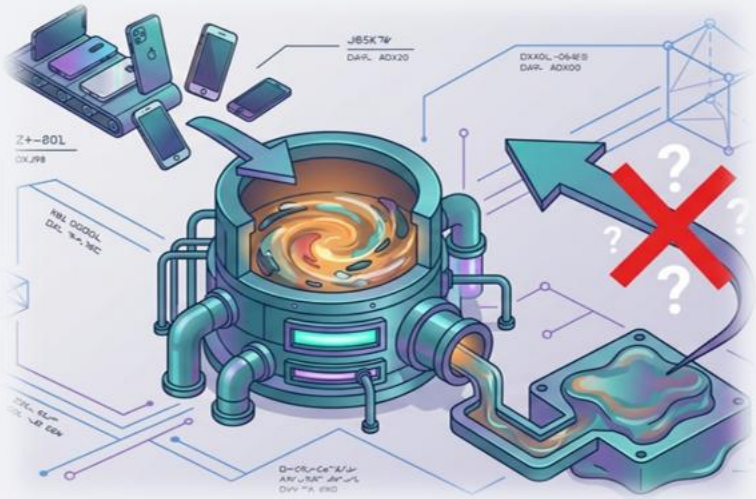
파쇄된 종이 뭉치 복구하기



아주 많은 파쇄된 종이 뭉치 속에서 조각들을 모아 원본 문서를 복원하는 것과 같은 복잡성입니다.

3. 해시 기반(Hash)

되돌릴 수 없는 용광로



용광로에 녹인 금속을 보고 원래의 제품 재료의 조합을 역추적하는 것은 불가능한 원리입니다.

대한민국 보안 자립의 이정표, KpqC

글로벌 표준(NIST)과 발맞추면서, 우리 IT 환경에 최적화된 독자 알고리즘으로 암호 주권을 확립합니다.

암호 주권(Crypto Sovereignty)

외산 암호 기술 의존 시 발생할 수 있는
기술 종속을 방지하고, 선진국에 전적으로
의지하지 않는 독자적인 암호 체계를 확립하여
기관의 핵심 데이터를 보호합니다.

국제 신뢰도(Global Trust)

세계적 수준의 국내 암호학계 기술력을 바탕으로
글로벌 시장에서의 영향력을 확대합니다.

민관 협력(Public-Private Synergy)

정부의 정책적 지원과 민간의 우수한 기술력이
결합하여 탄생한 K-암호 기술입니다.
특히 지식재산처는 글로벌 특허 빅데이터 분석을
통해 양자보안 기술의 초격차 특허전략을 수립합니다.

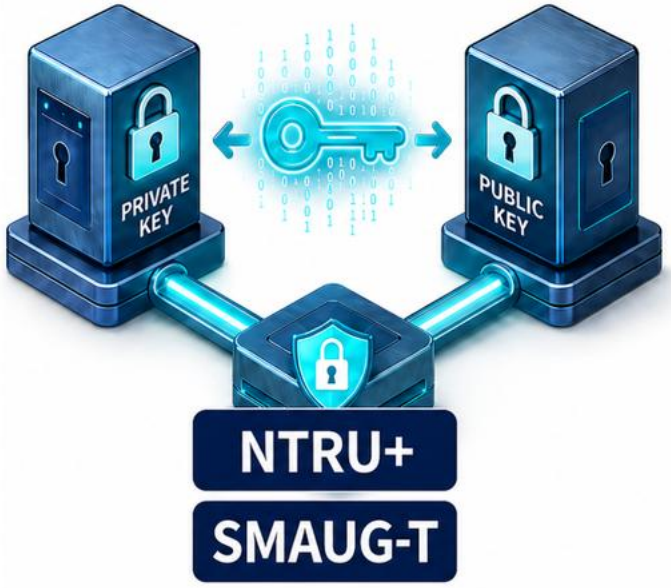
KpqC 핵심 알고리즘 라인업

전자서명

AIMer(대칭키) | SAMSUNG SDS KAIST

HAETAE(격자) | 서울대학교 SEOUL NATIONAL UNIVERSITY | HEAAN CRYPTO LAB

공개키암호 · 키설정



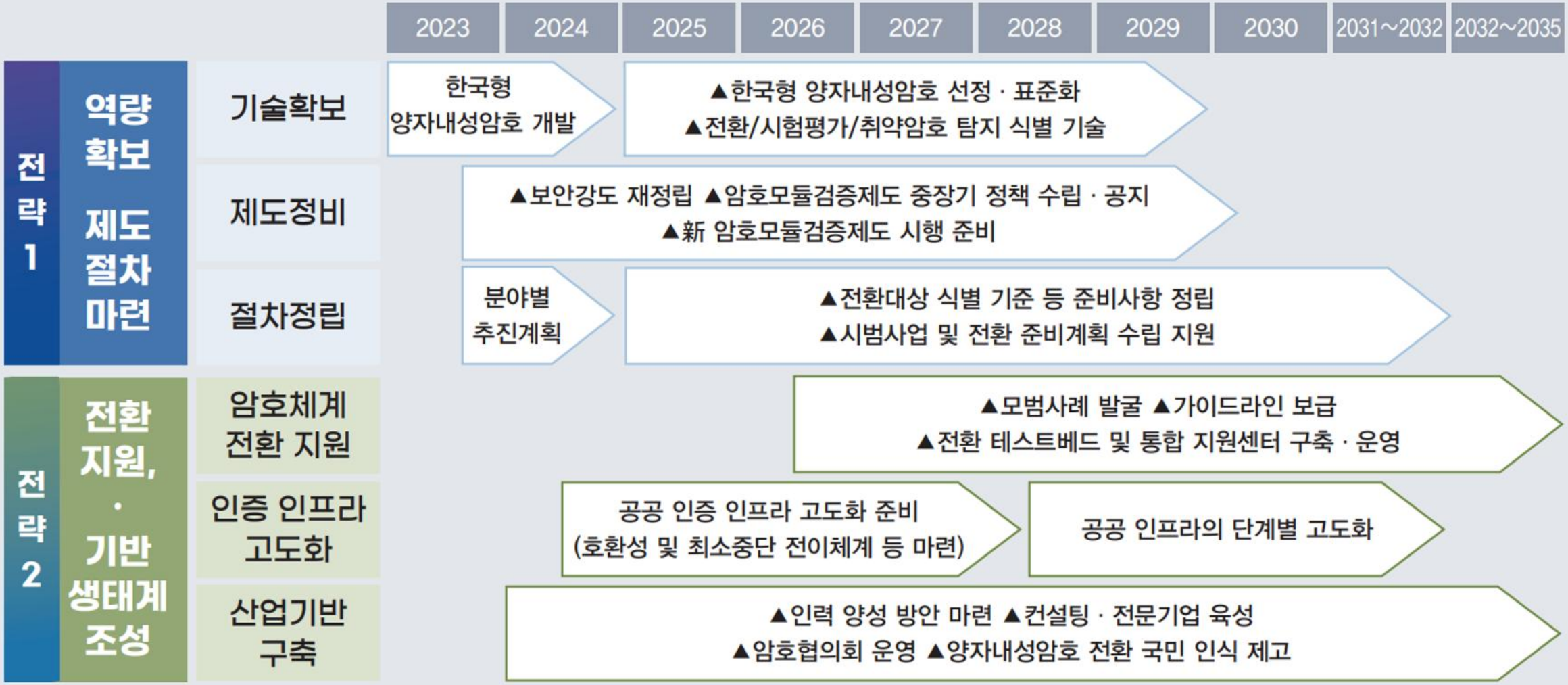
NTRU+(격자) | 상명대학교 SANGMYUNG UNIVERSITY 고려대학교 KOREA UNIVERSITY

SMAUG-T(격자) | 서울대학교 SEOUL NATIONAL UNIVERSITY | HEAAN CRYPTO LAB | 국군방첩사령부

Key Insights

한국은 격자 기반(SMAUG-T, HAETAE, NTRU+)과 대칭키 기반(AIMer) 알고리즘을 통해 균형 잡힌 KpqC 포트폴리오를 구축하고 있으며, 이를 바탕으로 글로벌 기술 표준을 선도하고 국가 안보를 강화할 것 입니다.

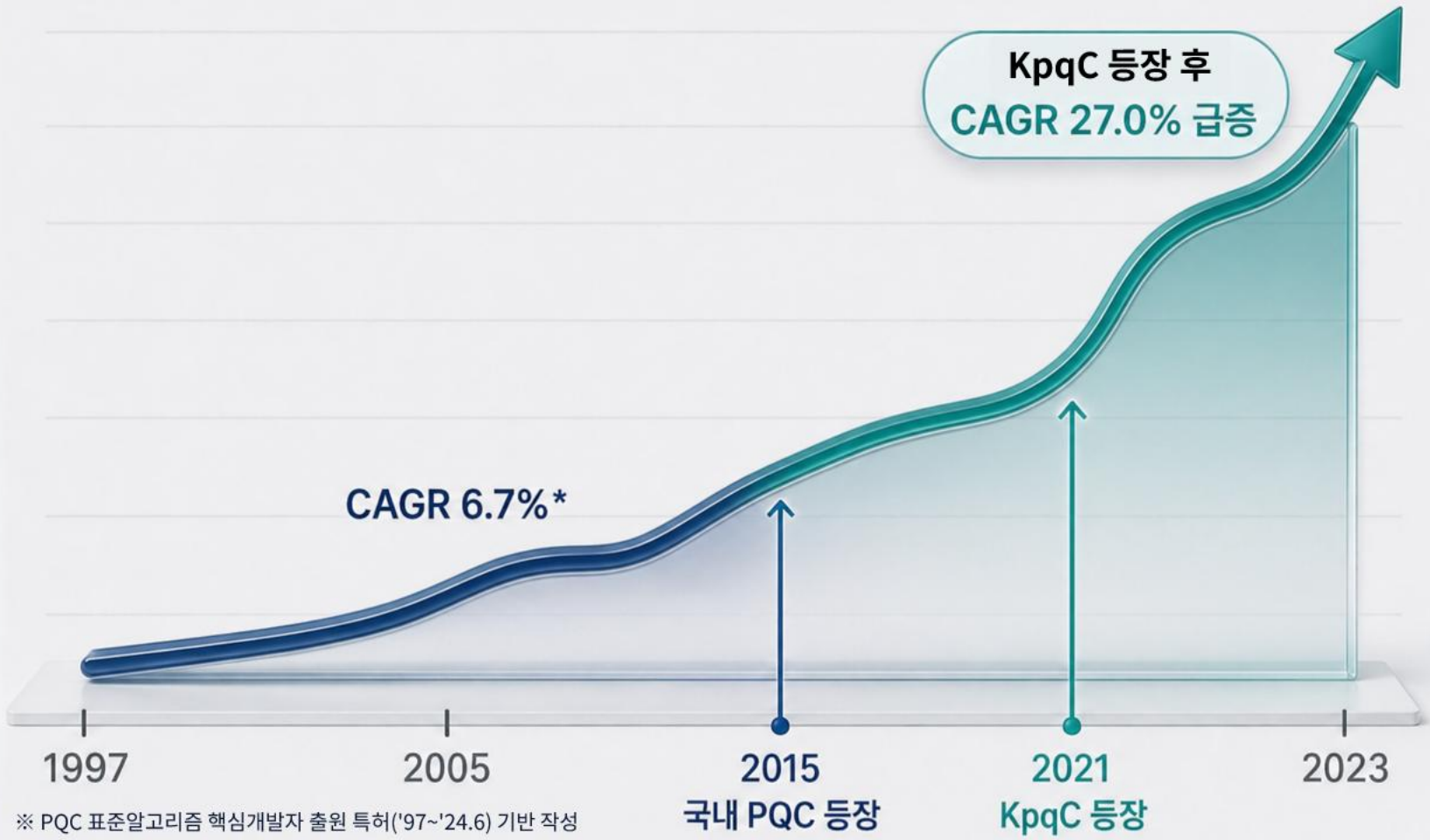
양자내성암호 전환 추진로드맵(요약)



※출처: 범국가 양자내성 암호체계 전환 종합 추진계획(2025.9)

폭발적인 PQC 특허규모 성장세와 한국의 역할

* CAGR(compound annual growth rate, 연평균성장률)



※ PQC 표준알고리즘 핵심개발자 출원 특허('97~'24.6) 기반 작성

Key Insights

지속적 증가
1997년 이후 PQC 특허 꾸준한 상승

국내 PQC의 모멘텀
2015년 국내 PQC 알고리즘의
본격적 등장으로 기술 혁신 가속화

국가별 위상
한국은 미국과 함께
세계 최상위권의 특허 출원 국가

데이터로 증명된 한국의 경쟁력: 알고리즘 점유율 분석

※ PQC 표준알고리즘 핵심개발자 출원 특허('97~'24.6) 기반 작성

Key Insights

- **압도적인 특허 활동**

  한국은 SMAUG-T(55건), HAETAE(53건) 등 격자 기반 알고리즘에서 가장 활발한 활동을 보임

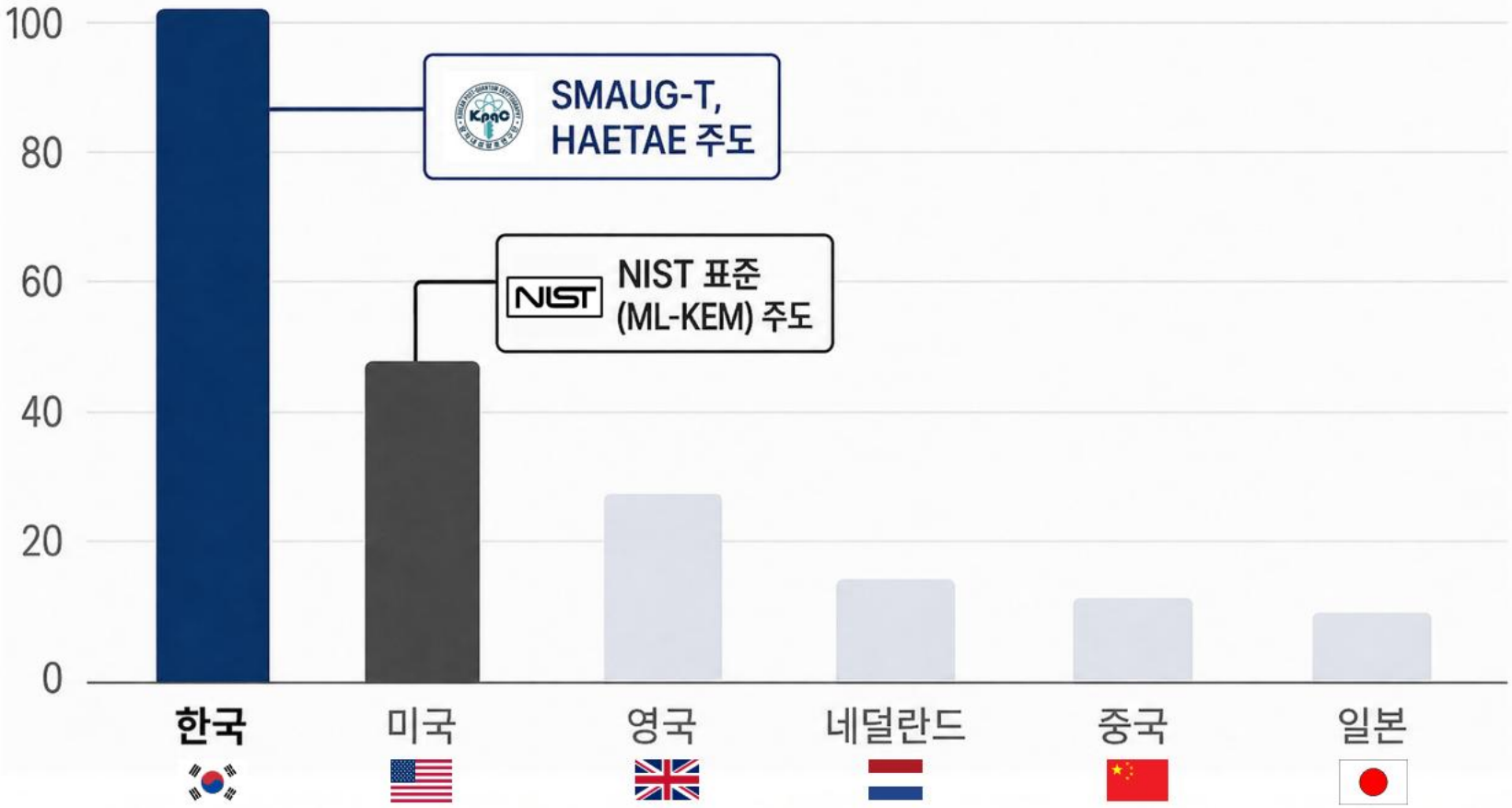
- **미국과의 경쟁**

  미국의 ML-KEM(49건)과 대등한 경쟁 구도 형성

표준알고리즘별 특허출원 규모 국가별 비교

대한민국(KpqC)과 미국(NIST)의 양강 구조 및 글로벌 기술 패권 경쟁

※ PQC 표준알고리즘 핵심개발자 출원 특허('97~'24.6.) 기반 작성

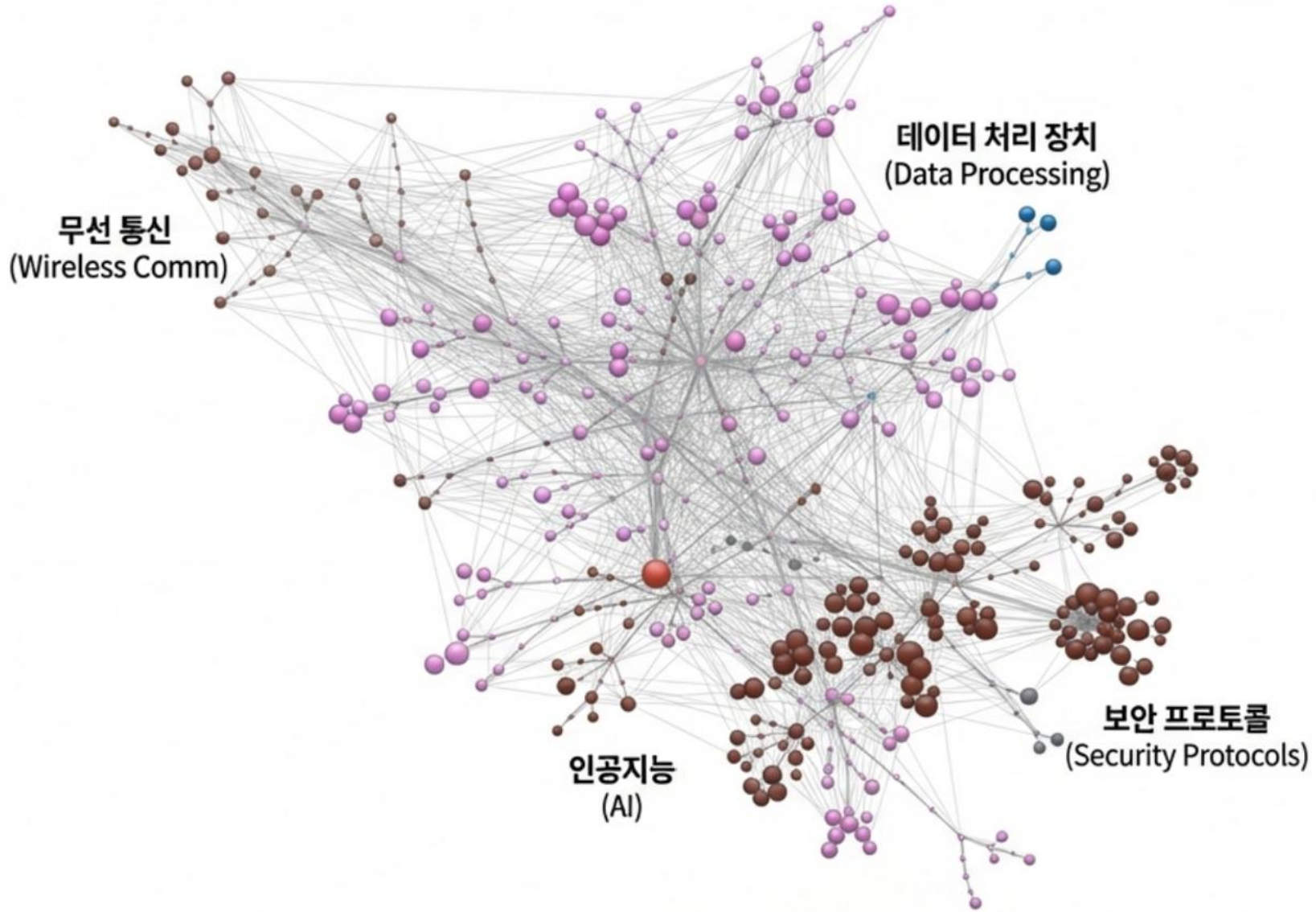


Key Insights

- **[양강 구도 형성]**
  한국은 격자 기반의 독자 알고리즘 (SMAUG-T, HAETAE)을 필두로 NIST 표준을 주도하는 미국과 대등한 수준의 특허 경쟁력을 확보함
- **[KpqC의 차별화]**
  미국 중심의 표준(ML-KEM)에 대응하여, 한국형 최적화 및 보안 주권 확보를 위한 독자 포트폴리오 구축 성공
- **[지속 성장세]**
  2015년 KpqC 등장 이후 연평균 **27%**의 폭발적인 특허 성장률을 기록하며 **세계 최상위권** 위상 유지

PQC의 활용·확산: 단순 보안을 넘어 산업 융합의 핵심으로

특허 인용 관계 분석으로 본 기술의 진화와 산업별 적용 현황



Key Insights

기술의 융합 (Convergence)

NIST 및 ISO/IEC 표준 특허 분석 결과, PQC 기술은 단순 암호화를 넘어 인공지능(AI) 및 데이터 처리(Big Data) 기술과 밀접하게 결합하며 고도화되고 있습니다.

응용 분야 확대 (Expansion)

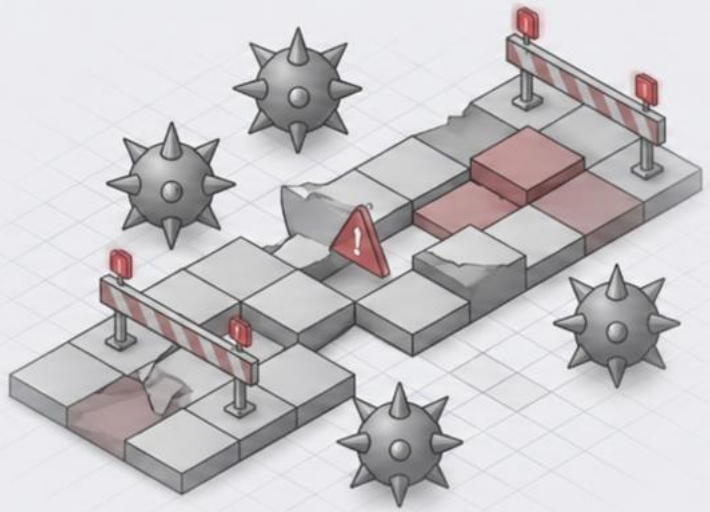
특허 인용 관계는 무선 네트워크(5G/6G), 금융(Fintech), 국방(Defense) 등 최고 수준의 보안이 요구되는 핵심 산업군으로 생태계가 급격히 확장되고 있음을 증명합니다.

보이지 않는 전쟁: 지식재산권(IP) 전략

특허 리스크를 두고 벌어지는 전쟁터 속에서, KpqC는 불필요한 로열티 부담과 분쟁 위험을 줄이며 기업의 안정적인 기술 활용을 지원합니다.

위험요소: 특허 분쟁과 비용

- **특허분쟁 리스크:** 글로벌 기술 선점 경쟁 심화로 인한 '특허 침해' 소송 가능성
- **비용 부담:** 해외 기술 의존 시 발생하는 막대한 로열티



IP전략: 기술 주권과 IP 보호의 핵심

- **기술 자생력 확보(Freedom to Operate, FTO):** 독자적인 K-PQC 원천기술 확보를 통해 자유로운 기술 활용 환경을 조성
- **비용 절감 및 로열티 방어:** 국산 암호 기술의 내재화로 해외 기술 의존도를 낮추고, 매년 발생하는 막대한 외화 로열티 지출을 차단

안전하고 독립적인 암호의 미래를 준비하십시오

Crisis: ‘Harvest Now, Decrypt Later’ 위협은 실재합니다.

Solution: KpqC는 검증된 기술력과 최적화된 성능을 제공합니다.

Safety: 철저한 FTO 분석으로 특허 분쟁 리스크를 줄인 안전한 양자 보안 생태계를 조성합니다.

지금이 바로 양자내성암호 체계로의 전환을 준비하고 대응해야 할 적기입니다.
대한민국 보안 주권, 귀하의 조직에서 시작됩니다.

지식재산처 양자내성암호연구단 한국특허기술진흥원