정보 보안

자가검증형 양자난수 생성 OTP 암호화 기술

소 속 재단법인 포항산업과학연구원 연구자 황혁기

기술 개요

◆ 제어 가능한 물리 모델로 양자 난수를 생성하고, 그 통계분포를 이론값과 대조해 신뢰성을 스스로 검증하는 자가검증형 양자난수 생성(QRNG) 기술로, 생성 난수를 일회용 패드(OTP)로 데이터를 암호화해 스마트제조·IoT 보안 플랫폼의 암호키 생성에 적용 가능

기존 기술 대비 차별성

기존 기술	본 기술
기존 QRNG는 엔트로피원의 물리 상태를 명확한 이론 모델로 예측·능동제어하기 어려워 편향이 생김	TFD(온도장 이중)·호킹온도 등 물리모델로 회전각을 정해 난수의 통계분포를 능동 제어
오작동·외부 공격이 발생해도 실시간 감지와 신뢰성 보장이 어려움	실측 분포를 이론분포(볼츠만/깁스)와 실시간 비교하는 자가검증으로 이상을 즉시 감지함
계산복잡도 기반 기존 암호(RSA·ECC)는 양자컴퓨터(쇼어 알고리즘)로 무력화될 위험이 있음	고신뢰 양자난수를 OTP로 XOR 암호화해 양자컴퓨터에도 안전한 정보이론적 보안을 제공함

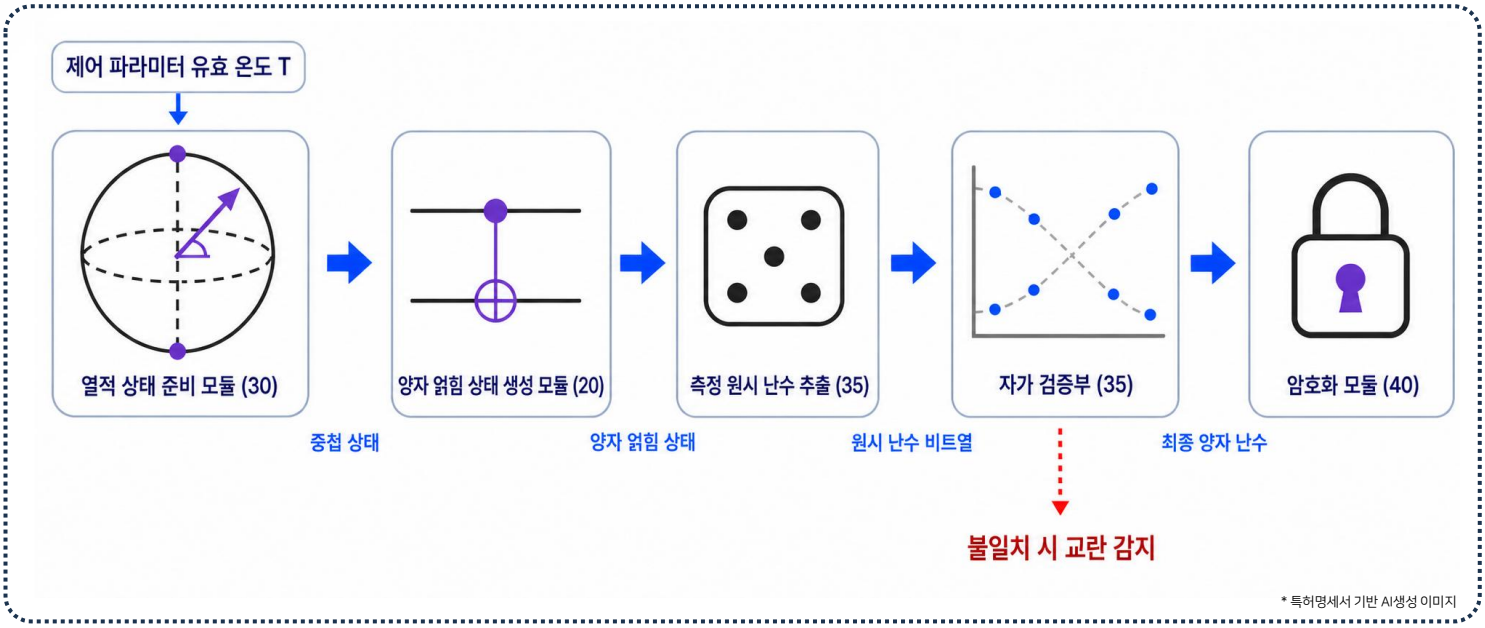
기술 특장점

물리모델 능동 제어
◆ 유효 온도(T)와 특성 에너지(E)로 회전각을 정해 엔트로피원의 열적 분포를 능동 제어함으로써, 기대되는 난수의 통계적 분포를 이론적으로 명확히 정의함

자가검증 내장 신뢰성
◆ 실측 분포를 이론분포(볼츠만/깁스)와 실시간 비교하는 자가검증(self-testing)으로 오작동·외부 교란을 즉시 감지하며, 최소 엔트로피는 NIST SP 800-90B 기준선 7.8 bits/byte를 안정적으로 상회

양자내성 OTP 보안
◆ 생성 난수를 일회용 패드(OTP)로 적용해 비트별 XOR 암호화함으로써 양자컴퓨터 공격에도 해독이 원천 불가능한 정보이론적 보안을 구현함

기술 개념도



* 특허명세서 기반 AI생성 이미지

정보 보안

자가검증형 양자난수 생성 OTP 암호화 기술

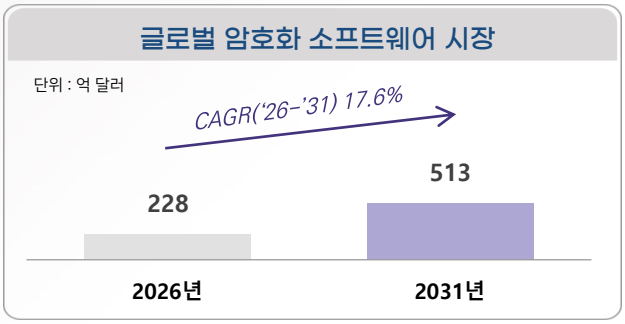
소 속 재단법인 포항산업과학연구원 연구자 황혁기

응용 분야

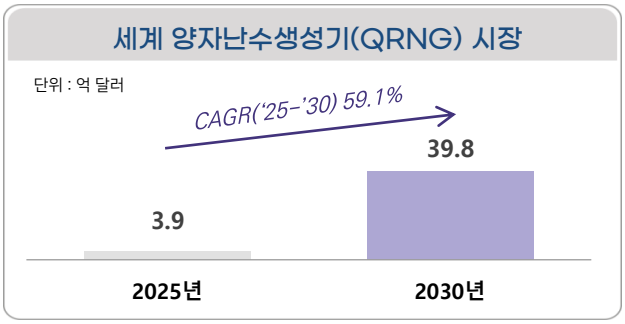
- **(스마트제조·산업데이터 보안)** 스마트공장 플랫폼 데이터의 권한·보안관리 등 산업제어 환경의 암호키 생성·데이터 보호에 적용
- **(IoT·모바일 기기 보안)** IoT·모바일 단말의 경량 QRNG 기반 암호키 생성과 통신 보안에 활용됨
- **(양자내성·국방/공공 고신뢰 보안)** 양자컴퓨터 공격에도 안전한 OTP 기반 고신뢰 키 생성과 기밀 데이터 보호에 적용

시장 전망 •산업동향

- **(산업 동향)** 양자컴퓨터의 기존 암호 위협(쇼어 알고리즘)이 부각되면서, 예측 불가능한 진성 난수를 물리적으로 생성·검증하는 QRNG와 양자내성 보안 수요가 빠르게 늘고 있음
- **(시장 전망)** 글로벌 암호화 소프트웨어 시장은 2026년 228.1억 달러에서 2031년 513.2억 달러로 연평균 17.6% 성장할 전망이며, 직접 시장인 글로벌 양자난수생성기(QRNG) 시장은 2025년 3.9억 달러에서 2030년 39.8억 달러 규모로 매년 59.1%씩 급성장 전망



* 출처 : Mordor Intelligence (2026)



* 출처 : The Business Research Company (2026)

구분	기업군	사업 분야	사업분야별 동향
1	대기업	양자암호 (QRNG·QKD) 통신	◆ 스위스 양자보안 전문기업을 인수하고 세계 최초로 모바일용 QRNG 칩을 상용화해 국내 프리미엄 스마트폰에 탑재함
2	중견	DB보안·데이터 암호화	◆ 본 특허 과제(플랫폼 데이터의 권한 및 보안관리 기술)를 수행하며 데이터 암호화 사업을 운영함('24 매출 약 118억원, 코스닥)
3	중소	QRNG반도체 (팹리스)	◆ 방사성 붕괴 기반 독자 QRNG 칩으로 FIPS 140-2 인증을 획득하고, 극한환경용 진성 난수 솔루션 공급과 국방 보안 프로젝트를 추진함

기술 성숙도 (TRL)



IP 정보

구분	특허번호	특허명	현재상태
1	10-2025-0133965	양자 난수 생성 장치, 이를 이용한 암호화 장치 및 그 방법들	등록