JIN INFRA

Quantum security 양자보안

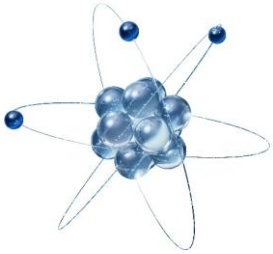
서비스영역
Service Area

암호기술의 현황과 양자 보안 기술의 핵심 개념, 해외 협력 업체 진행 현황, 그리고 진인프라의 양자 보안사업 전략 방향을 종합적으로 소개합니다. 양자컴퓨터의 급속한 발전은 현재의 암호체계를 근본적으로 위협하고 있으며, 이에 대응하기 위한 QKD와 PQC 기반의 차세대 보안 솔루션이 전 세계적으로 주목받고 있습니다. 산업 적용 가능성과 사업화를 위한 핵심 포인트를 한눈에 이해할 수 있도록 구성했습니다.

I. 암호기술

현대 암호체계의 구조와 활용 현황을 살펴보고, 공개키·대칭키 기반 보안의 역할과 한계를 정리합니다. 특히 양자컴퓨터 등장에 따라 발생하는 계산 복잡도 붕괴, 주요 위협 시나리오, 그리고 기존 인프라 전반에 미칠 영향을 함께 분석합니다.

II. 양자 보안 기술



QKD · PQC 핵심 기술 및 표준화 동향을 중심으로 차세대 보안의 원리를 설명합니다. 키 분배 방식, 알고리즘 전환 이슈, 상용화 수준, 그리고 국내외 표준화 움직임까지 함께 정리하여 기술 채택 시 고려해야 할 요소를 제시합니다.

III. 해외 협력업체

글로벌 양자보안 파트너 4사 현황을 비교하며 기술 역량, 협력 범위, 적용 산업, 사업 추진 단계 등을 요약합니다. 해외 레퍼런스와 협업 모델을 바탕으로 국내 적용 가능성과 시장 진입 전략을 함께 검토합니다.

IV. 진인프라 전략

양자산업 생태계 활성화와 사업 방향을 중심으로 진인프라의 역할을 구체화합니다. 기술 도입, 파트너십 확대, 레퍼런스 확보, 그리고 고객 맞춤형 솔루션 제안을 통해 시장 선점을 위한 실행 전략을 제시합니다.

JIN INFRA

I. 암호기술

암호기술 개요 및 양자 컴퓨터 위협

암호기술은 중요한 정보를 읽기 어려운 값으로 변환하여 제3자가 볼 수 없도록 하는 원천기술입니다. 크게 대칭키(AES, DES, SEED 등), 비대칭키(RSA, ECC), 해시함수(MD5, SHA), 전자서명(RSA, ECDSA)으로 분류됩니다. 각 방식은 용도와 보안 강도에 따라 다르게 적용되며, 양자컴퓨터 시대에는 이 중 상당수가 안전성을 잃게 됩니다.

암호 알고리즘별 양자 대비 현황

알고리즘	방식	양자 대비
AES	대칭키	키 길이 증가 필요
RSA	공개키	더 이상 안전하지 않음
SHA-2/3	해시	출력 길이 증가 필요
ECDSA/ECDH	공개키	더 이상 안전하지 않음
DSA	공개키	더 이상 안전하지 않음

양자컴퓨터 개발 동향

IBM(433큐비트·초전도), Google(Sycamore·초전도), Intel(실리콘 스핀), IonQ(32큐비트·이온트랩), Microsoft(위상 큐비트), AWS(Amazon Braket) 등 글로벌 빅테크 기업들이 경쟁적으로 양자컴퓨터를 개발 중입니다.

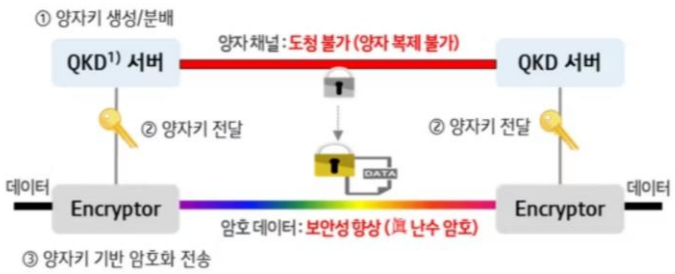
양자컴퓨터는 Shor 알고리즘(비대칭키 해독)과 Grover 알고리즘(대칭키 해독 단축)을 통해 현재 암호체계를 수초~하루 내에 해독 가능합니다. 기존 컴퓨터로는 백만 년이 소요되던 작업입니다.

II. 양자 보안 기술

암호기술 개요 및 양자 컴퓨터 위협

QKD – 양자 키 분배

양자역학 특성을 이용해 물리적으로 도청 불가능한 암호키를 분배합니다. BB84 프로토콜 기반으로 이론적으로 무조건적인 절대 보안이 증명되었습니다. 진난수(QRNG) 기반 암호키를 실시간 분배하며, 물리적 시스템으로 구현됩니다. 전송 거리 한계(약 90~120km)를 극복하기 위해 신뢰노드(Trusted Node)를 구성합니다.



PQC – 양자 내성 암호

양자컴퓨터로도 풀기 어려운 수학적 난제 기반으로 설계합니다. 격자(Lattice), 코드(Code), 해시(Hash), 다변수 방정식, 아이소제니(Isogeny) 등이 기반입니다.

- **미국(NIST) :** '22년 7월 CRYSTALS-KYBER, Dilithium, Falcon, SPHINCS+ 등 1차 표준 4종 발표
- **한국 :** 국정원 주관 KpqC 연구단이 '24년까지 국가표준 PQC 알고리즘 선정 예정

PQC 제품군은 ROADM 전송장비, PQC VPN, PQC LTE 라우터, PQC PUF USIM/eSIM 등으로 구성되며, 컴퓨터·서버·클라우드·모바일·결제·개인정보 등 다양한 영역에 Quantum Safe Migration이 가능합니다.

III. 해외 협력업체

양자보안 글로벌 파트너 & 진인프라 사업 전략

진인프라는 이스라엘·미국의 핵심 양자보안 기업 4곳과 전략적 협력 관계를 구축하고 있습니다. QKD와 PQC 분야의 최첨단 기술을 국내에 도입하고, PoC 테스트 및 파트너십 체결을 통해 양자보안 사업의 기반을 빠르게 확장하고 있습니다.

IL QuantLR (이스라엘, 2015) – QKD

- **방식 :** QKD (BB84 Decoy state)
- **제품 :** LoQomo1(100km), LoQomo2(40~60km), LoQomo3(5km)

타 QKD 장비(IDQ, Toshiba) 대비 가격 경쟁력 월등. 1:1 및 1:N 토폴로지 지원. 시에나 캐나다 오타와에서 전송장비 PoC 테스트 진행 중. 국정원 보안적합성 사전 검토 완료.

US QuSecure (미국, 2019) – PQC

- **방식 :** PQC (Saber, Kyber, BIKE, HQC)
- **제품 :** QuProtect™ (QuEverywhere, QuNetwork)

코드 변경 없이 TLS 위에 PQC 코팅 적용. TECHSLAYERS 인증, Accenture 우수기업 선정, 미 연방 정부 우수조달 제품 선정. Client PoC 테스트 완료, 파트너십 체결 진행 중.

US Quantum Xchange (미국, 2018) – PQC/QKD 통합

- **방식 :** PQC/QKD 통합 (IDQ 연계)
- **제품 :** PHIO TX(PQC+QRNG), PHIO TXD(양자 VPN), PHIO TXC(클라우드)

모든 NIST 후보 알고리즘 지원. 거리 제한 없음. ADVA, Ciena, Juniper, Cisco, Fortinet 등 주요 네트워크 장비와 호환. World Future Awards, Cyber Defense Magazine 수상.

US American Binary (미국, 2019) – PQC

- **방식 :** PQC (BFF 프로토콜, Kyber 1024 VPN)
- **제품 :** Fortress(SDN/SASE/Zero Trust), PQC Chat, PQC VPN, PQC PUF eSIM

Crypto-Agile SDN으로 미래 암호화 대비. 국방·헬스케어 분야 적용. Client PoC 완료, Fortress PoC 진행 예정.

IV. 진인프라 사업 방향

양자산업 생태계 활성화 및 4대 추진 전략

생태계 활성화 주요 내역

- **미래양자융합포럼(2021.06 발족) :** KT, SKT, LGU+, LG전자, 한국전력, 진인프라 등 산·학·연 참여
- **미래양자융합센터 MOU 체결(2023.08) :** 국내 양자산업 생태계 활성화 및 해외 진출 공동 추진 협약
- **의료·산업 구축 사례 :** A병원↔B병원 42km QKD 기반 실시간 의료 협진, 산업용 로봇 IoT에 QRNG 적용한 36km 관제 시스템 구축
- **2023 글로벌 교류 프로그램(2기) :** 미국 워싱턴 QWC 컨퍼런스, QED-C, IonQ, Fairfax County EDA 방문 (22명 대표단)

4대 사업 추진 방향

시범사업 확대

QKD/PQC → Hybrid 방식, 1:1 → 1:N, N:N으로 확대하여 투자비 절감

기술경쟁력 확보

글로벌 QKD·PQC 벤더 협력, 국내 기관 인증을 통한 해외 기술력 습득

Local 컨설팅 선점

24시간 365일 양자 컨설팅 제공, 망설계·구축·운용 종합 기술지원

홍보 및 교육 강화

양자주간·양자의날 부스 운영, 초·중·고·대학교 대상 양자 중요성 홍보