11장. 최신 ICT 보안기술

퀀텀컴퓨팅과 차세대 퀀텀 AI의 미래

박종혁

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech ac kr

Contents 목차

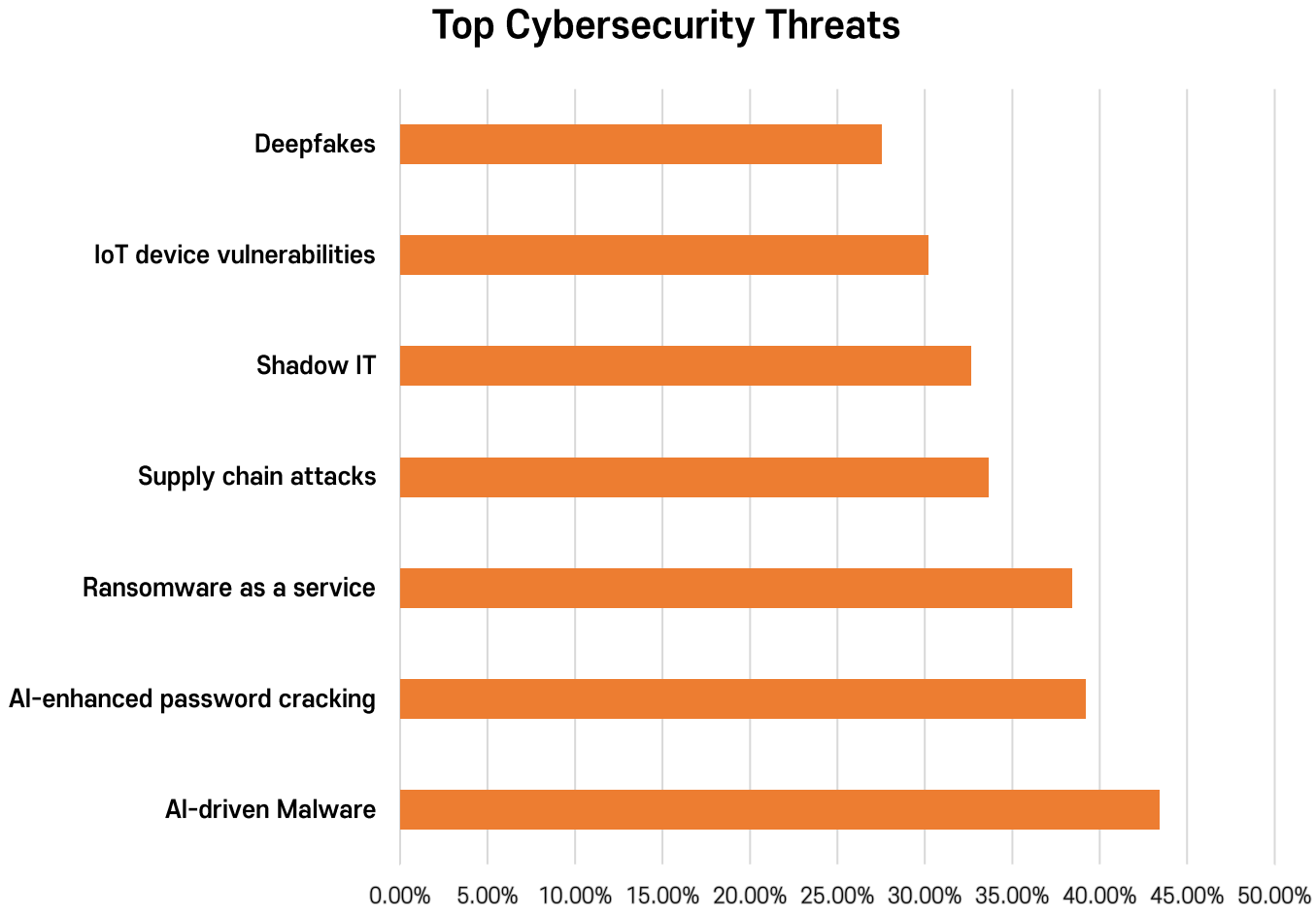
1. 서론

AI와 퀀텀의 만남

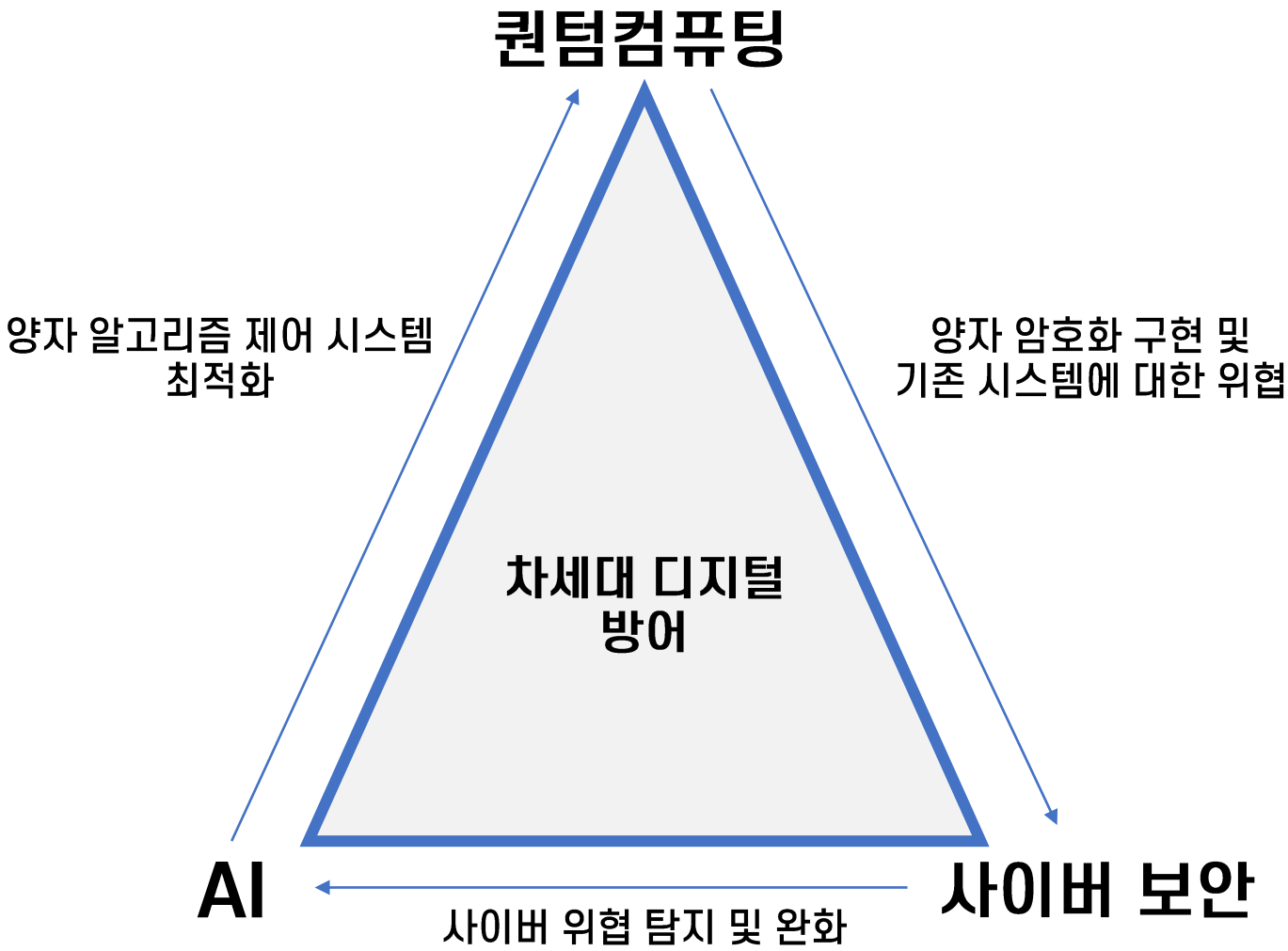
- 전 세계 기술혁신을 이끄는 두 축 : 인공지능(AI) + 퀀텀 컴퓨팅(QC)
  - ✓ 국가 전략과 글로벌 경쟁 구도의 핵심
- 산업 전반을 변화시키는 AI는 데이터 기반 학습 + 지능형 의사결정으로 구성
  - ✓ 제조·금융·의료·교통 등 모든 산업의 자동화와 효율화를 주도
- 불가능을 가능케 하는 퀀텀 컴퓨팅 : 현대 컴퓨터의 한계 돌파
  - ✓ 복잡한 최적화, 신약 개발, 암호 해독 등 초고난도 문제 해결에 활용
- AI × 퀀텀의 결합 = 보안·금융·헬스케어·국방 인프라 혁신
  - ✓ 양자내성암호, 위협 탐지, 초고속 데이터 분석으로 새로운 패러다임 전환을 촉진

AI와 퀀텀컴퓨팅의 융합

- **새롭게 부상하는 위협 트렌드**
  - ✓ AI 악성코드(43.4%), 비밀번호 크래킹(39.2%), 서비스형 랜섬웨어(38.4%), 딥페이크(27.5%)가 주요 위협
- **양자 기반 위협의 부상과 복합 공격 시나리오**
  - ✓ 부채널 공격·AI 피싱·딥페이크·자동화 악성코드 생성 등 새로운 공격 벡터가 등장
- **보안 패러다임 변화 : PQC + QKD + AI 기반 탐지**
  - ✓ 기존 RSA·ECC는 양자에 취약하며, 각국은 PQC와 양자 안전 솔루션에 투자
- **PQC의 필요성과 국제 표준화 동향**
  - ✓ NIST PQC 프로젝트가 진행 중이며, Kyber·Dilithium이 차세대 표준 후보로 채택
- **미래형 보안 전략 = AI × QC의 상호 보완적 역할**
  - ✓ 실시간 지능형 탐지와 양자내성암호를 결합해 금융·헬스케어·국방 인프라 보호



[주요 사이버 보안 위협]

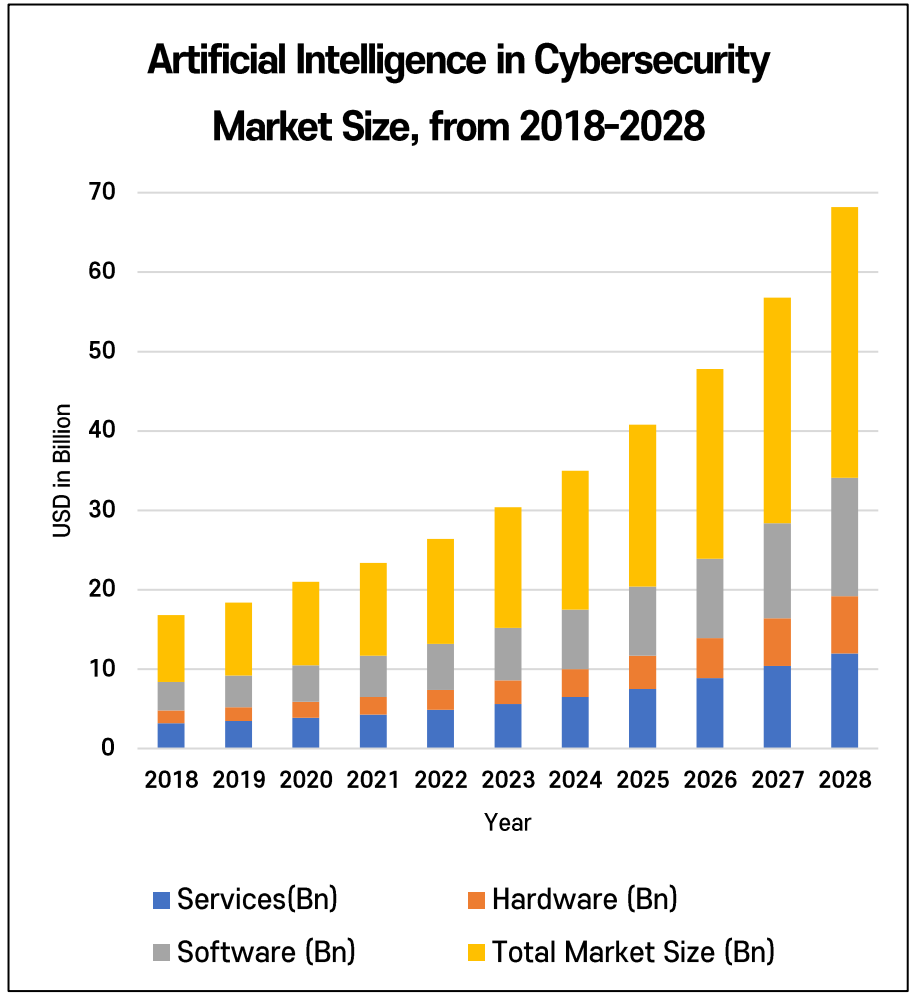


[AI·퀀텀컴퓨팅·사이버 보안 기반 차세대 디지털 방어]

2. AI 및 QC 산업·연구 동향

사이버 보안의 AI 및 퀀텀 응용

- **AI 기반 보안 프레임워크의 진화**
  - ✓ NIST 사이버 보안 프레임워크(CSF 2.0)
    AI 이상 탐지를 통합하고 AI 리스크 관리 프레임워크 (AI Risk Management Framework, AI RMF)로 안전한 도입 가이드 제공
- **AI로 강화되는 위협 인텔리전스**
  - ✓ IBM Watson은 NLP로 위협 정보를 자동 분류해 보안 대응 속도 향상
- **양자 안전 로드맵과 AI 결합**
  - ✓ IBM zSystems와 클라우드에 PQC 및 고급 AI를 적용해 차세대 보안 전략 추진
- **보안 자동화의 확산**
  - ✓ MITRE ATT&CK은 AI 기반 자동화를 통해 TTP 시뮬레이션과 공격·방어 훈련 가속화
- **새로운 위협 모델의 부상**
  - ✓ 보호·공격용 AI 에이전트, DeepLocker와 같은 자가 적응형 악성코드 주목
- **글로벌 시장 성장 전망**
  - ✓ 사이버보안 AI 시장 - 2028년까지 571억 달러 규모로 성장, 탐지·분석·자동화 분야에 필수



[사이버보안 AI 시장 규모 : 2018-2028]

AI 성숙도 - 유형별 국가 분포 by BCG

- AI 보안 글로벌 컨설팅기업인 **보스턴컨설팅그룹(BCG)**

  전 세계 73개국을 대상으로 AI 성숙도 조사

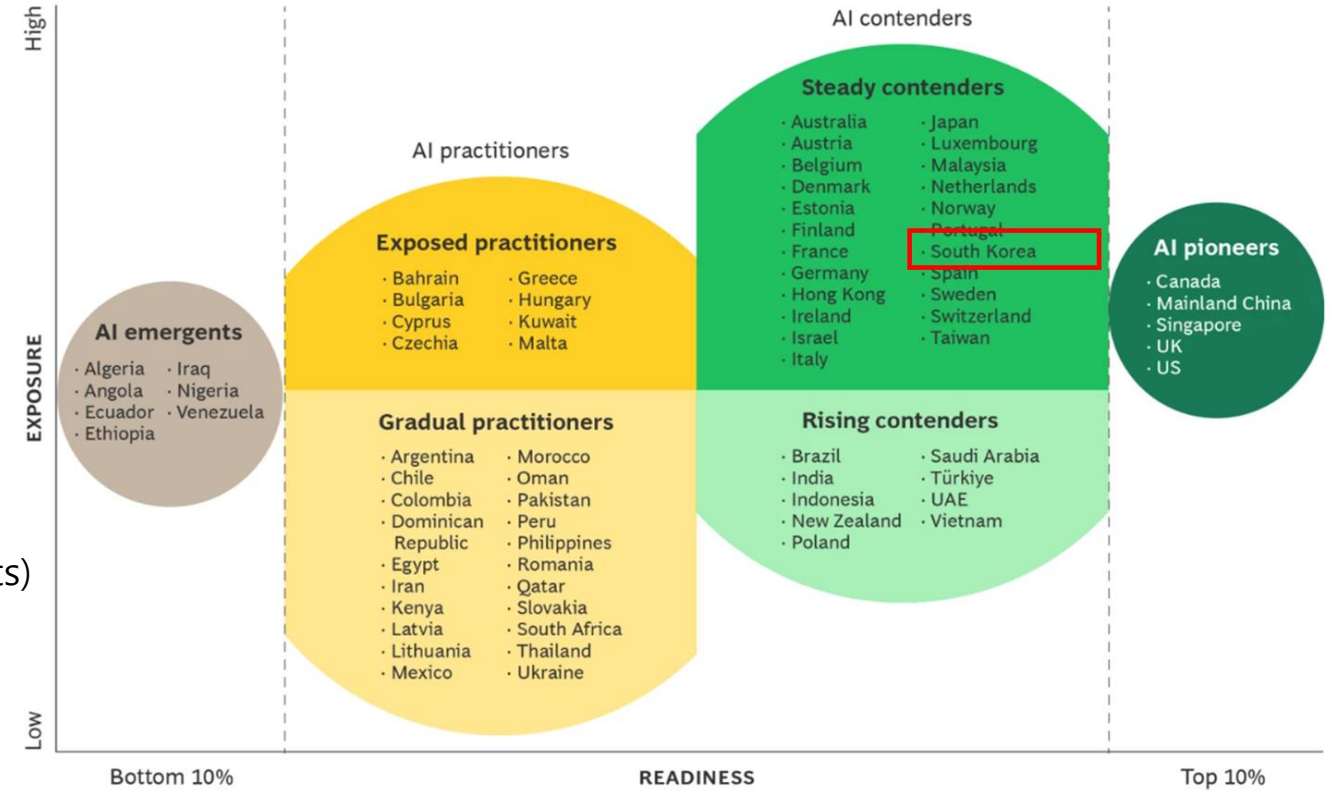
  ✓ **정부의** AI **기술 전담 조직 존재 여부,** AI **전문가의 집중도,** AI **유니콘 기업가치 등 다양한 지표 활용**

- 4**그룹 분류**

  AI **선도국** (Pioneer) -**안정적 경쟁자** (Steady contenders)

  - **취약한 실천국** (Exposed practitioners) - **도약단계** (Emergents)

- **한국 - 안정적 경쟁자 그룹**



대형언어모델(LLM)과 생성형 AI의 보안 활용

- **공격 - 자동화된 레드팀 활동**
  - ✓ GPT 계열 모델은 피싱 이메일, 맞춤형 악성코드, 코드 스캔을 통한 공격 효율성 극대화
- **방어 - 블루팀 워크플로우 최적화**
  - ✓ 로그 요약, 사고 분류, SOAR 스크립트 생성, 위협 리포트 자동화 활용
- **보안 운영 혁신**
  - ✓ GPT-4-Turbo, IBM Granite 등 - SIEM 규칙 매핑과 플레이 북 자동화
  - ✓ Microsoft Defender Copilot - LLM을 통합한 위협 탐지 및 대응 자동화
- **보완책 필요**
  - ✓ LLM은 여전히 jailbreak 공격에 취약, 악성 지시 수행 가능성 존재
  - ✓ AI 방화벽, 머신 러닝, 책임성 확보가 차세대 방어 체계의 핵심 과제로 부상

퀀텀컴퓨팅 연구 동향과 주요 성과

[산업계]

기업	주요 성과	특징
IBM	Quantum System One, Quantum System Two, Condo (1,121 큐비트), Heron (156 큐비트) 발표	2025년까지 4,000 큐비트 달성 목표
Google	Sycamore, Bristlecone, Willow 칩, 105 큐비트 기반 무작위 회로 샘플링	현대 컴퓨터 대비 1만 년 → 5분 수준 격차 증명
IonQ	Forte 시스템, Quantum OS 제공	클라우드 기반 트랩 이온 접근, 하이브리드 서비스로 오버헤드 100배 감소
중국	Jiuzhang - 광자 양자 컴퓨터 성과	특정 연산에서 현대 컴퓨터 능가, 초전도·광자 방식 병행 연구

[학계]

- 오류 보정 및 알고리즘 최적화 연구
  - ✓ 동적 회로, 회로 연결 기반 오류 완화 기술과 새로운 양자 알고리즘 설계 활발히 진행

[공통 연구 방향]

- 서버리스 런타임, 오류 완화, 실용적 오류 보정으로 상용화 가능성 확대

● '양자 우위'에서 '양자 이점'으로

- Google - 2019 년, 53 큐 비 트 의 Sycamore 프로세서를 이용한 무작위 회로 샘플링 실험을 통해 '양자 우위' 달성 주장
- IBM - 기존의 고성능 컴퓨터로 며칠 내에 동일한 결과를 얻을 수 있다며 이 주장에 이의 제기

→

- Google Willow (2024) - 임계값 이하의 오류 보정과 초지수적인 속도 향상주장, 오류 스케일링 성능 개선
- 이에 대한 활발한 논의가 있었지만 실제 결함 허용 수준에는 미치지 못함

→

- D-Wave Advantage2 (2025) - 어닐링 방식을 통해 자기 물질을 시뮬레이션하는 데 있어 실용적인 우위를 확보했다고 주장 (해당 계산을 20분만에 수행)
- 이는 기존 컴퓨터로 약 100만 년이 걸릴 문제를 효과적으로 해결한 것이지만, 학계 논쟁 지속 중

↓

- 현재 연구 분야 - '양자 우위'에서 벗어나 최적화, 화학 및 ML 등의 실제 응용 분야에서 의미 있는 성능 향상을 달성하는 '양자 이점'으로 초점 이동

→

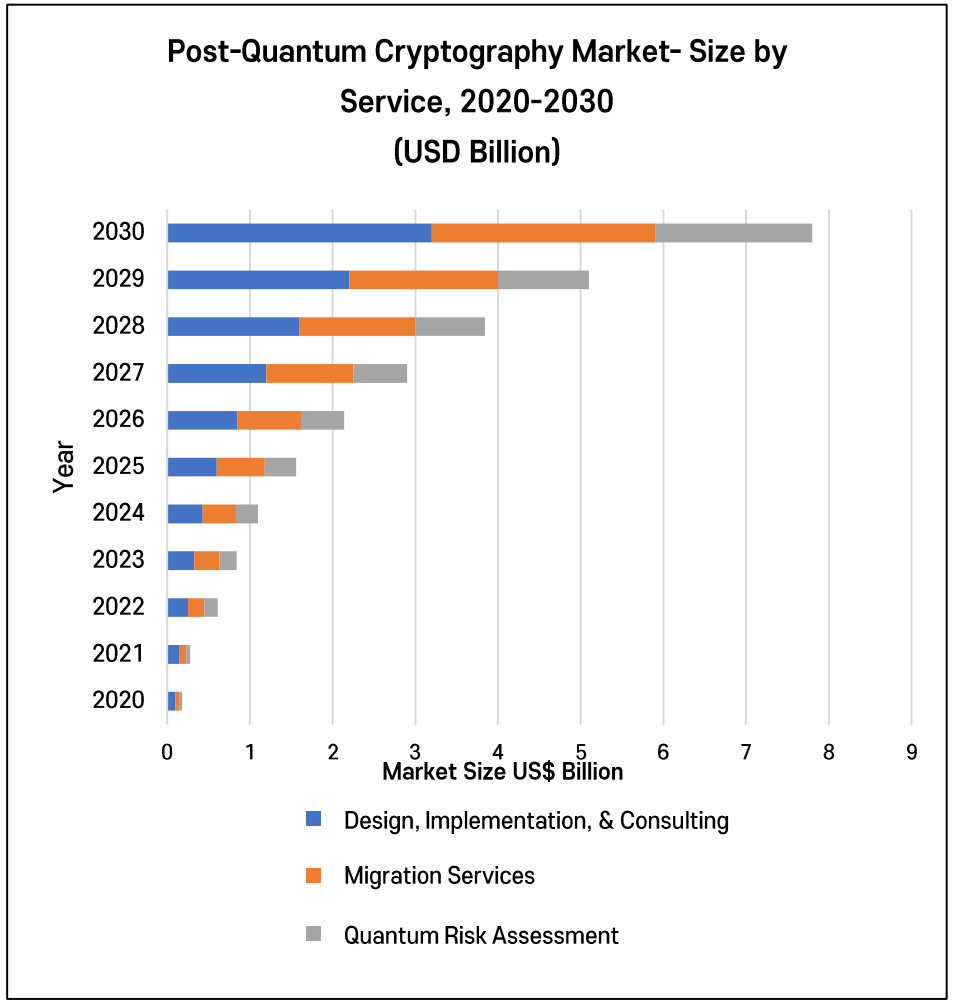
- 칼텍(Caltech) - 양자 성능을 보다 현실적으로 평가할 수 있도록 새로운 벤치마크 기준 제안

→

- IBM과 Quantinuum과 같은 다른 플랫폼 - 논리 큐비트 및 시스템 연결성 측면에서 주요 성과 보고

PQC 표준화 동향

- **NIST PQC 최종 승인 (2024)**
  - ✓ Kyber (FIPS 203), Dilithium (FIPS 204), SPHINCS+ (FIPS 205)
- **백업 알고리즘 채택 (2025)**
  - ✓ HQC가 코드 기반 KEM 후보로 추가, 최종 표준화는 2027년 예정
- **산업계 적용 확산**
  - ✓ Google Chrome, Microsoft, AWS가 하이브리드 암호 시스템을 서비스에 도입
- **클라우드·플랫폼 통합 확대**
  - ✓ IBM, Google, Microsoft는 Windows·Azure·Chrome·HSM에 PQC 통합
- **인터넷 트래픽 전환 가속화**
  - ✓ Cloudflare 기준, 전체 트래픽의 16%가 이미 PQC 기반 키 교환 활용 중
- **시장 성장 전망**
  - ✓ PQC 시장은 2024년 11.5억 달러에서 2030년까지 연평균 37.6% 성장할 것으로 예상



[서비스별 양자내성암호 시장 규모 : 2020-2030]

3. AI 및 QC 응용 시나리오

핀테크 트랜잭션 보안의 AI 응용

- **AI 통합 핀테크 보안 모델**
  - ✓ 핀테크 시스템에 AI을 통합하여 거래 보안성, 사기 방지, 운영 자동화 향상 방안 제시
  - ✓ 예측 기반 위협 분석, 실시간 이상 탐지, 지능형 인증 모델 등 포함
- **ML과 블록체인을 활용** - 대규모 금융 데이터셋 분석, 학습 기반 모델, 변조 불가능한 분산 검증 적용
- **행동 기반 실시간 사기 탐지**로 무단 거래를 차단, 오탐률 감소 및 속도 향상
- **예측 모델링의 효과** - 위협 발생 이전 선제 대응 가능, 재정적 피해 최소화로 신뢰성 강화
- 정리 – AI는 금융 서비스에 대한 신뢰성과 안정성을 크게 강화
  - ✓ AI는 핀테크 보안에서 단순히 위협을 탐지하는 것을 넘어,
  - ✓ 예측·차단·자동화까지 아우르는 종합적 보안 체계로 발전

의료·헬스케어: 연합학습 및 PQC기반 데이터 보호

- **하이브리드 보안 모델 연구**
  - ✓ 연합학습 및 격자 기반 PQC로 환자 데이터 보호 모델 제시

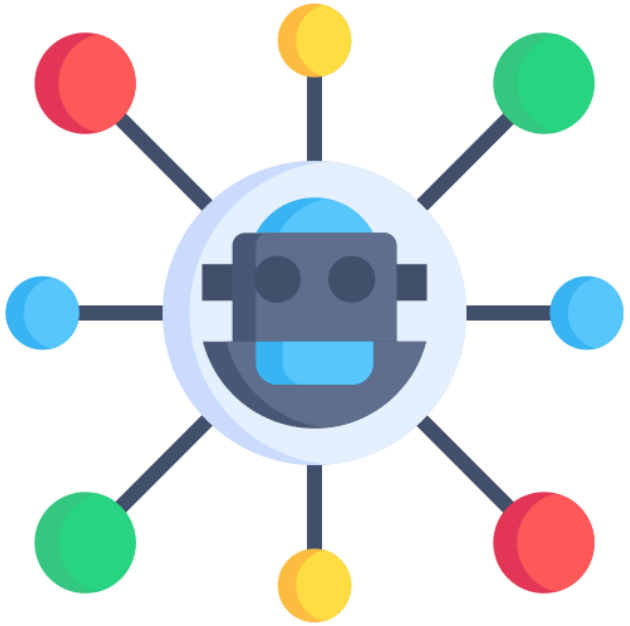
- **보안 설계 요소** - LWE 기반 암호로 FL 업데이트 보호, Kyber/Dilithium을 키 교환 · 엣지 인증에 적용

- **연합학습 아키텍처** - 클라이언트는 로컬 데이터로 학습, 격자형 암호화로 QC 환경의 복호화 불가 보장

- **성능 및 보완점**
  - ✓ 웨어러블 시뮬레이션에서 강력한 프라이버시 보장
  - ✓ 대규모 임상 배포에는 하드웨어 가속화 및 최적화 필요
- **정리**
  - ✓ 연합학습과 PQC의 결합은 의료 데이터 보호의 새로운 패러다임을 열며,
  - ✓ 프라이버시 보장과 양자 안전성을 동시에 달성할 수 있는 핵심 전략

사물인터넷: 경량 AI+양자내성암호로 보안 강화

- **적응형 AI 보안 프로토콜 개발**
  - ✓ AI 기반 IDS를 통해 위협 예측·이상 탐지·실시간 방어 최적화
  - ✓ PQC 통합으로 키 교환 안전률 증가, 격자 및 다변수 암호 기법으로 양자 공격 대응
- 연합학습, 차등프라이버시, 동형암호, 엣지 AI로 민감 데이터 보호 및 전송 부담 최소화
- **양자-현대 하이브리드 보안 모델 개발**
  - ✓ QKD, PQC, 양자 머신러닝(QML) 통합 하이브리드 보안 모델 - 이상 탐지 정확도 향상, 지연시간 감소, 오탐률 감소로 기존 방식 대비 성능 대폭 향상
- **추가 고려사항** - PQC 구현의 연산·메모리 오버헤드, 배터리 제약, 불투명한 AI 신뢰성 문제 등
- **정리**
  - ✓ IoT 환경 보안은 단순히 AI만이 아니라 AI, PQC, QML이 결합된 하이브리드 접근을 통해
  - ✓ 성능과 안전성을 동시에 달성하는 방향으로 발전



4. AI 및 QC 전략·트렌드

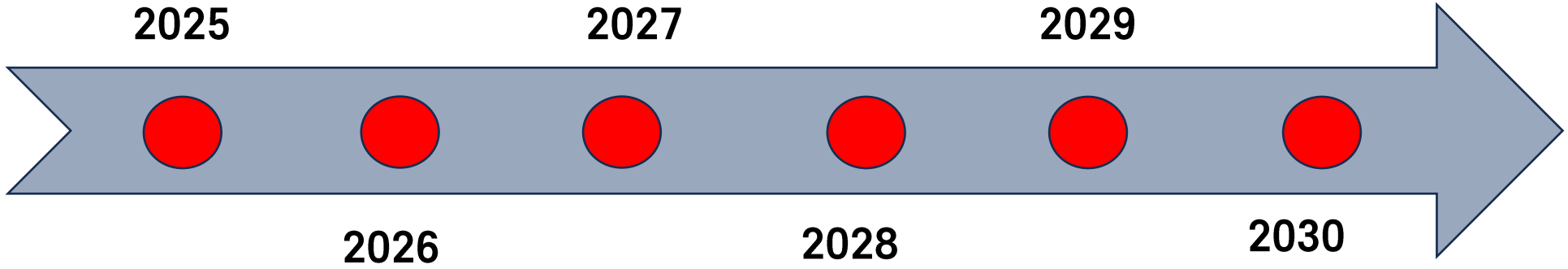
빅테크 기업과 국가 전략

- **Google**
  - ✓ 2019년 Sycamore 프로세서로 '양자 우위' 달성 선언
  - ✓ Chrome & BoringSSL에 PQC 키 교환 기본 적용 - 사용자 트래픽 보호
- **IBM**
  - ✓ 2033년까지 10만 큐빗 양자컴퓨터 구축 목표
  - ✓ 클라우드 중심 생태계 및 양자 안전 솔루션 확산
- **Microsoft**
  - ✓ 하이브리드 모델 : 현대암호 + PQC
  - ✓ Azure Key Vault, AD CS, Intune 등 핵심 인프라 서비스에 PQC 통합
- **국가 전략 연계**
  - ✓ 미국 NIST PQC 표준화 (2024) - 글로벌 산업 전환 촉진
  - ✓ 유럽 · 아시아 주요 국가 - Q-Day 대비 로드맵 수립 중
- **정리**
  - ✓ 빅테크 기업과 각국 정부 모두 - 양자 보안과 PQC 도입을 선제적으로 추진, 미래 경쟁력 확보를 위해 노력

“Q-Day” 대비 양자내성암호 전환

- Q-Day : 양자컴퓨터가 현재 사용되는 암호화 기술을 해독할 수 있는 충분한 성능에 도달하는 시점
  - ✓ 기존 보안 체계의 전면적 재편이 필요한 시점
  - ✓ 지식재산권, 국가 기밀, 금융 기록과 같이 장기간 가치가 유지되는 모든 민감 데이터가 현재 위험 노출

위협 : "지금 수집하고 나중에 복호화" (Harvest Now, Decrypt Later, HNDL)



Today

이미 암호화된 데이터

탈취/저장

공격자

Future

강력한 양자컴퓨터를 확보 후,
복호화 계획

PQC 전환의 클라우드 제공자 역할

- AWS, MS Azure, Google Cloud

제공업체	주요 PQC 전략	주요 전환 리소스
AWS	핵심 보안 서비스에 선제적으로 통합 및 하이브리드 PQC를 통한 전송 중인 데이터 보호	• 마이그레이션 계획서 • 실습형 워크숍 • 오픈소스 코드 패키지
Microsoft Azure	ID, 인증서, 플랫폼 인프라 전반에 걸친 종합적 통합 및 개발자 프리뷰	• 사전 접근 빌드(Windows Insiders) • SymCrypt 라이브러리 • 파트너 컨설팅 서비스(OZ Digital)
Google Cloud	핵심 인프라에 적극적으로 배포하고 오픈소스 도구 제공 및 개발자 지원	• 전문가 가이드(CISO 사무국) • 오픈소스 라이브러리 • 광범위한 기술 문서

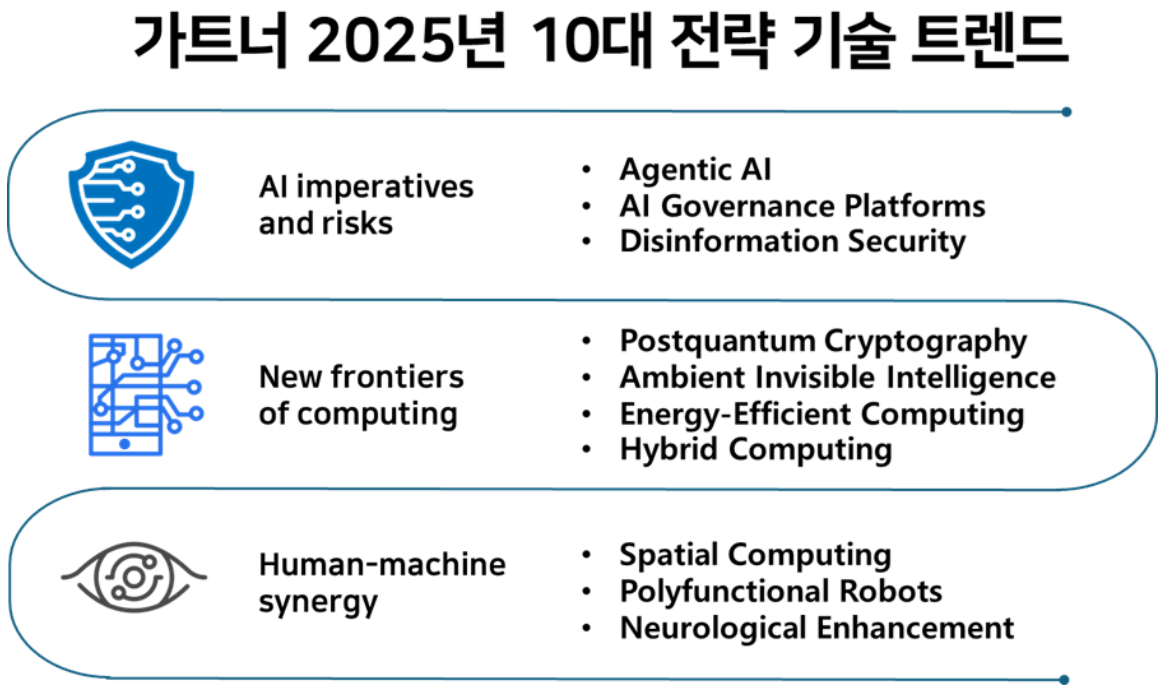
✓ PQC 전환의 핵심 동력으로 기업보안 전략과 긴밀히 연계

PQC 클라우드 보안 프레임워크

- 격자 기반 암호와 적응형 AI를 결합하여 다중 클라우드 인프라에서 **선제적 보호 프레임워크** 개발
- 양자 위협 및 현 컴퓨팅 환경의 한계 - RSA, ECC, ElGamal 암호는 Shor(쇼어) 알고리즘에 취약
- **격자 기반 암호**
  - ✓ SIS·LWE 기반으로 양자 공격에 안전
  - ✓ Kyber, Dilithium, FrodoKEM 등 적용
  - ✓ SIMD기반 하드웨어 가속으로 10배 성능 향상 및 낮은 에너지 소비
- **보안 아키텍처 통합**
  - LBC, ZKP, **QKD 통합 및 AI 기반** 이상 탐지를 통합한 **블록체인 지원 클라우드 보안 강화**
- **추가 고려 사항**
  - AI 기반 키 수명주기 관리 및 실시간 위험 평가
  - 경량, 모듈화, 제로트러스트 기반 암호 생태계 확산

가트너 2025 전략 기술 트렌드 – AI/QC 기반

- **AI 중심 기술**
  - ✓ 10대 전략 기술 중 9개 AI - Agentic AI, AI 거버넌스, Disinformation Security 등
  - ✓ 2028년까지 최소 15% 업무 자율 처리 예상
- **뉴 컴퓨팅 패러다임**
  - ✓ 공간 컴퓨팅(AGI·로봇), 주변 비가시성, 지능(스마트홈·스마트팩토리), 하이브리드 컴퓨팅 (에너지 효율 + 다기능 로봇)
- **양자 관련 트렌드**
  - ✓ PQC: AI 외 유일한 비AI 분야
    - ➔ Q-Day 대비 필수 보안 기술
- **글로벌 기업·정부 차원의 선제적 도입 가속화**



[가트너 2025년 10대 전략 기술 트렌드]

퀀텀 AI 시대에 요구되는 보안 프레임워크

- **무엇을 했는가?**

  ✓ NIST - 수년에 걸친 글로벌 협력을 통해 PQC 알고리즘 포트폴리오를 선정하고 2024년에 최종 표준 확정

표준 (FIPS 번호)	알고리즘 이름	암호학 기능	주요 사용 사례	기반 수학
FIPS 203	ML-KEM (CRYSTALS-Kyber)	키 캡슐화 매커니즘	TLS, VPN과 같은 보안 통신 프로토콜에서의 공유 비밀키 설정	구조화된 격자
FIPS 204	ML-DSA (CRYSTALS-Dilithium)	디지털 서명 알고리즘	데이터와 소프트웨어의 진위 및 무결성 검증	구조화된 격자
FIPS 205	SLH-DSA (SPHINCS+)	디지털 서명 알고리즘	암호학적 다양성을 제공하는 백업 서명으로 표준화	해시 함수

[NIST Post-Quantum Cryptography Standards (NIST FIPS 203/204/205)]

- **어떻게 할 것인가?**

  ✓ MITRE - PQC 전환을 위해 단계별 로드맵을 통해 기업을 위한 실질적인 4단계 전략 제시

  - 준비 (Preparation) : 이해관계자의 동의를 얻고 책임자 지정
  - 기초 이해 (Baseline Understanding) : 모든 암호화 자산을 식별하고 목록 작성
  - 계획 및 실행 (Planning & Execution) : 맞춤형 마이그레이션 계획 수립 및 예산 편성
  - 모니터링 및 평가 (Monitoring & Evaluation) : 진행 상황 추적 및 복원력 유지

5. 결론

- **AI/퀀텀는 차세대 컴퓨팅 기술 혁신의 핵심 축**
  - ✓ 사이버 보안, 금융, 헬스케어, 국방 등 핵심 인프라의 근본적 변화 제시
  - ✓ 데이터 처리 속도와 보안 수준을 동시에 혁신적으로 향상
  - ✓ 글로벌 경쟁 구도의 전략적 우위를 결정하는 핵심 동력

- **AI/퀀텀이 여는 미래 사회와 산업적 기회**
  - ✓ 초고속 의사결정 및 최적화로 신약 개발, 스마트시티, 에너지 분야 가속화
  - ✓ 국가 안보, 금융 시장 안정성 및 의료 진단 정확도 등 산업적 기회 확대
  - ✓ AI/퀀텀은 사회 전반의 디지털 전환을 가속화하는 성장 엔진

- **AI/퀀텀 시대의 보안 전략**
  - ✓ 양자 위협에 대응하기 위해 PQC와 AI 보안 프레임워크 결합 필요
  - ✓ 클라우드, IoT 및 엣지 환경의 적응형 AI 기반 보안 모델 도입 강화
  - ✓ PQC 적용을 통한 안전한 키 교환 및 제로 트러스트 아키텍처 모델 도입

6. 참고문헌

참고문헌

1. Statista. (2023). Artificial intelligence (AI) in cybersecurity market size worldwide from 2018 to 2028. Statista

2. Grand View Research. (2025). Post-Quantum Cryptography Market | Industry Report, 2030. Grand View Research

3. Goffer, M. A., Uddin, M. S., Hasan, S. N., Barikdar, C. R., Hassan, J., Das, N., ... & Hasan, R. (2025). AI-Enhanced Cyber Threat Detection and Response Advancing National Security in Critical Infrastructure. Journal of Posthumanism, 5(3), 1667–1689.

4. Bayya, A. K. (2025). Implementing AI-Driven Transaction Security Protocols and Automation in Next-Gen FinTech Solutions. Asian Journal of Mathematics and Computer Research, 32(1), 104-132.

5. He, X., Xu, G., Han, X., Wang, Q., Zhao, L., Shen, C., ... & Feng, D. (2025). Artificial intelligence security and privacy: a survey. Science China Information Sciences, 68(8), 1-90.

6. Kasula, V. K., Rakki, S. B., & Banoth, R. (2025, May). Enhancing Hyperledger Fabric Security with Lightweight Post-Quantum Cryptography and National Cryptographic Algorithms. In 2025 37th Conference of Open Innovations Association (FRUCT) (pp. 93-99). IEEE.

7. Commey, D., & Crosby, G. V. (2025). PQS-BFL: A Post-Quantum Secure Blockchain-based Federated Learning Framework.

8. Rakhshanda, M., & Iqra, A. (2025). AI-Enhanced Secure Communication Systems for Next-Generation IoT Networks: Protocols, Threat Mitigation, and Quantum Resilience. Spectrum of Engineering Sciences, 3(2), 925-94.

9. Gartner. (2025). Top Technology Trends 2025.

10. Panda Security. (2025). 9 Key Cybersecurity Trends to Know in 2025 [New Data]. Panda Security.

11. Cherukupalle, N. S., & Cherukupalle, N. (2025). Quantum-Resilient Cloud Systems: Preemptive Shielding Against Post-Quantum Cryptographic Threats. Journal of Information Systems Engineering and Management, 10(38s), 1234-1246.

참고문헌

12. Liu, C. Y., Chen, S. Y. C., Chen, K. C., Huang, W. J., & Chang, Y. J. (2025). Federated quantum-train long short-term memory for gravitational wave signal.

13. Faris, K., Al-Shareeda, M. A., Abbood, A. A. J., Almaiah, M. A., & AlAli, R. Quantum-Enhanced AI and Machine Learning: Transforming Predictive Analytics.

14. The AI Maturity Matrix, BCG, 2024

감사합니다

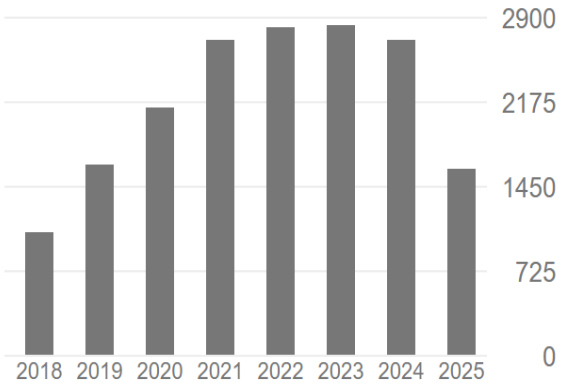
서울과학기술대학교 박종혁 교수
(Email : jhpark1@seoultech.ac.kr)

부록

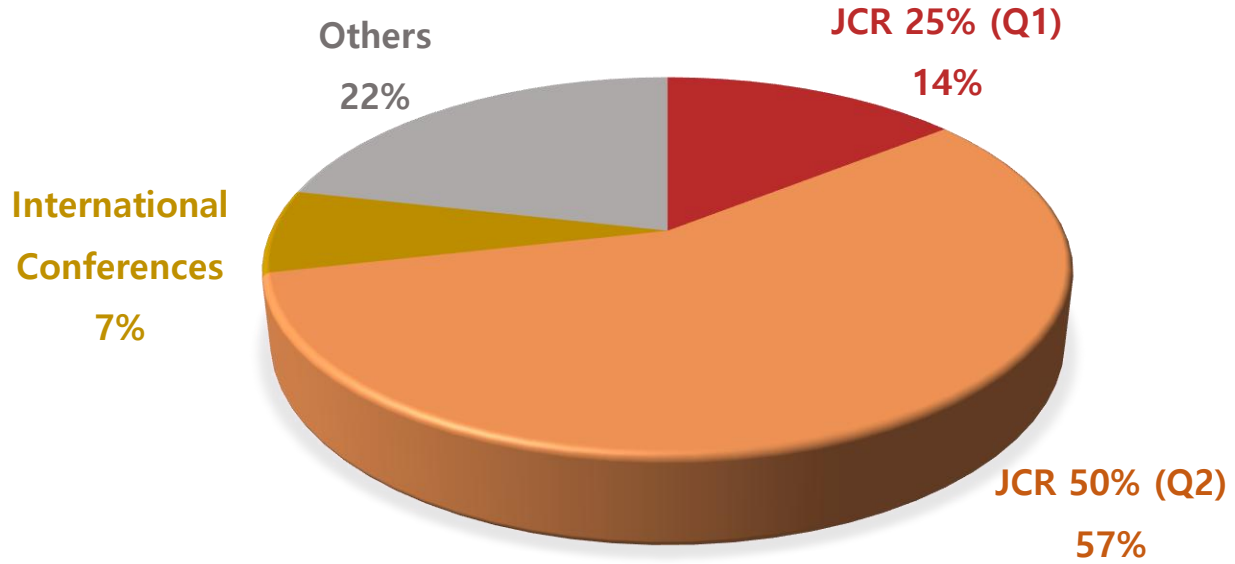
Jong Hyuk Park

SeoulTech, Dept. of Com. Sci. & Eng.
Verified email at seoultech.ac.kr - Homepage
AI Security IoT Blockchain Quantum

	전체	2020년 이후
서지정보	21566	14896
h-index	70	60
i10-index	314	197



PAPERS AND RESEARCH PUBLICATIONS



- 최근 5년간 JCR 1% 저널인 Information Fusion을 포함하여 JCR 상위 25% 저널에 70편 이상의 논문을 발표하였으며, 총 약 500여편의 SCIE 저널 논문 게재
- Google Scholar 기준 **총 인용 수는 21,566회, h-index 70, i10-index 314 기록**
- AI 보안, 퀀텀 보안, IIoT 보안 기술, 데이터 보호, 분산형 인공지능 모델 등 다양한 보안 기술 분야에서 **총 21건의 특허(출원/등록) 보유**
- 미국 스탠포드 대학에서 발표하는 **"세계 과학자 상위 2% 연구자"에 2024년까지 7년 연속 선정**

연구 분야

퀀텀
사이버 보안

인공지능 보안

블록체인

네트워크/IoT 보안

프로젝트 현황

프로젝트명	연구지원기관	사업기간	총사업비	프로젝트 설명
안전한 통신 네트워크를 위한 블록체인기반 위임 양자 클라우드 기반기술 연구	한국연구재단	2022.12.26~ 2025.12.25	1,500,000,000원	디바이스 간 인증 및 안전한 클라우드 서비스를 위한 블록체인 Q-OTP·Quantum Machine Image 알고리즘 및 프로토콜 개발
안면인식 CCTV에서 동일 주체 연결분석 가능한 실시간 얼굴 비식별화 기술	한국인터넷진흥원	2023.04.01 ~ 2025.12.31	3,418,000,000원	안면인식 CCTV 환경의 개인정보 보호와 동일 인물의 연결 분석을 위한 AI 기반 얼굴 검출, 가상 얼굴 변환, 엣지 디바이스 실시간 처리, 복수 영상 간 연결·추적, 병렬 영상 처리 기술 개발
지속 가능한 유·무선 통신 네트워크 서비스를 위한 퀀텀 머신러닝 기반 안전하고 효율적인 사이버 보안 공격 대응 기술 개발	한국연구재단	2023.07.01 ~ 2026.06.30	900,000,000원	지속가능한 IIoT 서비스 제공을 위한 퀀텀 머신러닝 알고리즘 및 AI 등 첨단 기술을 활용한 사이버 보안 공격의 대응 기술 개발
IT&OT 융합 제어시스템의 안전한 운영을 위한 신뢰성 있는 AI 기반 사이버 공격 탐지 기술 개발	한국산업기술진흥원	2024.10.01 ~ 2027.09.30	1,500,000,000원	IT&OT 융합 제어시스템의 안전한 운영을 위한 효율적이고 신뢰할 수 있는 AI 기반 사이버 공격 탐지 기술 개발

박종혁 교수

주소 : 서울특별시 노원구 서울과학기술대학교 미래관 325호

연구실 전화 : 02-970-6702

휴대 전화 : 010-9036-4042

이메일 : jhpark1@seoultech.ac.kr

홈페이지 : https://jamespark.seoultech.ac.kr