사물인터넷융복합논문지 Vol. 12, No. 3, pp. 131-142, 2026 https://doi.org/10.20465/KIOTS.2026.12.3.131

휴머노이드 로봇 PQC 클라우드 보안 아키텍처의 예비 타당성 분석 연구

장상현[1], 박동성[2], 김동주[3*]
[1]국가첨단백신개발센터 책임연구원, [2]국가첨단백신개발센터 연구원, [3]대구가톨릭대학교 컴퓨터소프트웨어학부 교수

A Preliminary Feasibility Study on Post-Quantum Secure Cloud Architecture for Humanoid Robots

Sang-hyun Jang[1], Dong-seong Park[2], Dongju Kim[3*]
[1]Ph.D., Senior Researcher, Korea Advanced Center for Vaccine Development
[2]Researcher, Korea Advanced Center for Vaccine Development
[3]Professor, School of Computer Software, Daegu Catholic University

요 약 휴머노이드 로봇과 Physical AI 시스템이 클라우드 기반 AI 서비스에 의존함에 따라, 로봇-클라우드 통신 보안은 데이터 보호를 넘어 물리적 안전 보장의 핵심 요소로 부상하고 있다. 기존 RSA 및 ECC 기반 공개키 암호는 양자 컴퓨팅 환경에서 Shor 알고리즘에 취약하며, HNDL(Harvest-Now, Decrypt-Later) 공격은 인간 행동 데이터의 장기 기밀성을 위협한다. 본 연구는 NIST FIPS 203 표준인 ML-KEM-768 기반 양자내성 키 교환과 AES-256-GCM 인증 암호화를 결합한 하이브리드 PQC 보안 아키텍처의 적용 가능성을 분석하였다. 특히 ML-KEM의 NTT 기반 O(n log n) 연산 구조가 RSA의 $O(n^3)$ 모듈러 지수 연산 대비 ARM 임베디드 환경에 구조적으로 적합함을 이론적으로 고찰하였다. 또한 PC환경 기준 음성(10KB), 이미지(1MB), LiDAR 포인트 클라우드(10MB) 데이터에 대한 AES-256-GCM 암호화 지연을 측정·분석한 결과, 모든 모달리티에서 실시간 요구사항을 만족하였으며 deadline miss가 발생하지 않았다. ARM Cortex-A72 환경에 대해서는 문헌 기반 추정을 통해 실시간 요구사항 충족 가능성을 예비적으로 확인하였다. 더불어 MITM, HNDL, 세션 하이재킹, 액추에이터 명령 변조를 포함한 위협 모델과 Hybrid TLS/PQC 기반 단계적 전환 방안을 제시하였다. 본 연구는 preliminary feasibility-oriented investigation 수준의 아키텍처 연구이며, 향후 Jetson Orin NX 기반 실물 검증과 ROS2 통합을 수행할 예정이다.

주제어 : 양자내성암호, ML-KEM, 휴머노이드 로봇, 클라우드 보안, ARM 임베디드, HNDL 대응

Abstract As humanoid robots and Physical AI systems increasingly rely on cloud-based AI services, robot-cloud communication security has become a safety-critical requirement beyond conventional data protection. Existing RSA- and ECC-based public-key cryptography is vulnerable to quantum attacks, particularly Shor's algorithm, while harvest-now-decrypt-later (HNDL) threats endanger the long-term confidentiality of human behavioral data. This study investigates the applicability of a hybrid Post-Quantum Cryptography (PQC) architecture combining ML-KEM-768(NIST FIPS 203) for quantum-resistant key exchange with AES-256-GCM for authenticated encryption. We theoretically analyze the suitability of ML-KEM for ARM-based embedded environments, highlighting the efficiency of NTT-based O(n log n) polynomial operations compared with RSA's $O(n^3)$ modular exponentiation. Experimental latency measurements on a PC baseline platform for audio, image, and LiDAR point cloud data indicate that all modalities satisfy real-time constraints without deadline miss. For ARM Cortex-A72 environments, literature-informed estimates suggest the potential to meet real-time requirements, pending direct hardware validation. In addition, threat models including MITM, HNDL, session hijacking, and actuator command tampering are discussed, together with a practical Hybrid TLS/PQC migration path. This work represents a preliminary feasibility-oriented architectural investigation, with future work planned for Jetson Orin NX deployment and ROS2 integration.

Key Words : PQC, ML-KEM, Humanoid Robot, Cloud Security, AES-256-GCM, ARM Cortex, HNDL

*교신저자 : 김동주(deekim@cu.ac.kr)
접수일 2026년 05월 29일 수정일 2026년 06월 19일 심사완료일 2026년 06월 22일

1. 서론

휴머노이드 로봇은 Boston Dynamics의 Atlas, Agility Robotics의 Digit 등으로 대표되는 바와 같이 단순 물리적 자동화 시스템을 넘어, 클라우드 기반 인공지능 서비스와 긴밀히 결합된 Cyber-Physical AI 시스템으로 발전하고 있다[1]. 이러한 휴머노이드 로봇은 인간과의 직접적 상호작용이 증가함에 따라 사회적·물리적 안전에 대한 요구사항도 함께 높아지고 있다.

음성 인식, 시각 인식, 행동 계획 등 고차원 인지 기능은 로컬 온보드 연산만으로는 처리하기 어려우며, 클라우드 서버와의 지속적인 실시간 데이터 교환에 의존한다[2]. 이 구조는 로봇–클라우드 통신 채널을 시스템 신뢰성과 안전성의 핵심 경계(critical security boundary)로 만든다.

기존 보안 패러다임은 주로 데이터 기밀성에 집중해 왔으나, Cyber-Physical AI의 부상은 이 패러다임을 근본적으로 재정의하고 있다. 통신 채널의 침해는 단순한 정보 유출을 넘어 물리적 피해로 직결될 수 있기 때문이다. MITM 공격자가 로봇의 제어 명령을 변조할 경우 액추에이터 오작동이 발생하며[3,4], 나아가 AI 명령이 인체 신경근육계를 직접 제어하는 Physical AI 환경에서는 통신 보안 실패의 영향이 한층 심화될 수 있다. 아직 이를 입증한 동료심사 연구는 부재하나, EMS 기반 인체 제어 시연[28]과 같은 초기 개념 검증 사례는 이러한 위협 표면의 확장 가능성을 예시적으로 보여주는 참고 자료로 볼 수 있다. 이러한 맥락에서 Cyber-Physical AI 시스템의 통신 보안은 단순한 정보 보호를 넘어, 물리적 안전 보장을 위한 핵심 요구사항으로 재정의될 필요가 있다.

HNDL(Harvest-Now, Decrypt-Later) 공격의 위협은 장기적 관점에서 고려되어야 한다. 휴머노이드 시스템은 운용 과정에서 음성·영상·행동 로그 등 방대한 인간 행동 데이터를 지속적으로 축적하며, 이 데이터는 장기간 암호화된 형태로 클라우드에 저장·전송된다[14].현재의 RSA/ECC 기반 암호화로 보호된 이 데이터는 미래의 양자 컴퓨터에 의해 소급 복호화될 위험에 노출되어 있으며, 이는 오늘 수집되는 데이터의 장기 프라이버시 노출 문제를 야기할 수 있다[11]. IBM의 1,121큐비트 Condor 프로세서, Google의 surface code 오류율 감소 성과 등 양자컴퓨팅의 급속한 진전은 이러한 위협의 현실화 시점을 앞당기고 있다[24,25].

이러한 배경에서 본 연구는 휴머노이드-클라우드 통신 환경에서 PQC 기반 보안 아키텍처의 필요성과 적용 가능성을 분석하는 것을 목표로 한다. 본 연구는 실물 배포 전 단계의 '아키텍처 예비 타당성 조사'로서, 선행 문헌 기반 분석을 통해 보안 메커니즘의 이론적 적합성과 실시간성 확보 가능성을 입증하는 데 집중한다. 구체적인 연구 목표는 다음과 같다.

C1. Cyber-Physical AI 관점에서 휴머노이드 환경에서의 PQC 필요성을 물리적 안전 보장을 위한 핵심 요구사항으로 재정의한다.

C2. ML-KEM 기반 경량 세션 키 교환 아키텍처를 설계하고, 이에 대한 이론적 연산 효율성을 분석한다.

C3. 데이터 모달리티 특성을 고려한 암호화 구조와 데이터 유형별 worst-case latency bound를 분석한다.

C4. ARM 기반 임베디드 환경에서의 적용 가능성을 예비 수준에서 평가하고, 단계적 Hybrid PQC migration 경로를 제시한다.

2. 관련연구

2.1 휴머노이드–클라우드 통합과 보안 공격 표면

휴머노이드 로봇의 클라우드 연동은 일반적으로 ① Cloud-based SLAM, ② 원격 딥러닝 추론, ③ Federated 행동 학습의 세 가지 기능 영역을 중심으로 이루어진다[2]. 이러한 구조는 로봇 기능을 서비스 형태로 제공하는 RaaS(Robot as a Service) 모델로 확장되고 있으며, 인간-로봇 상호작용(HRI) 환경에서 로봇의 자율성과 통신 신뢰성은 핵심 요구사항으로 인식되고 있다. Kehoe et al.(2015)은 클라우드 로보틱스의 주요 장점으로 연산 오프로딩(computation offloading), 대규모 데이터 활용, 집단 학습(collective learning)을 제시하였다[2]. 그러나 동시에 네트워크 의존성 증가에 따라 보안 공격 표면(attack surface)이 확대될 수 있음을 지적하였다. 실제로 클라우드 기반 로봇 시스템은 센서 데이터, 제어 명령, 학습 모델이 지속적으로 네트워크를 통해 교환되므로, 통신 구간이 주요 공격 대상이 될 수 있다. 로봇 시스템의 보안 취약점에 관한 연구도 지속적으로 수행되어 왔다. Quarta et al.(2017)은 산업용 로봇 컨트롤러에 대한 체계적 보안 분석을 통해 원격 코드 실행(remote code execution) 및 제어 명령 변조 가능성을 실증하였다[3]. Cheng et al.(2022)은 ROS2 기반 환경에서 TLS가 적용되지 않을 경우 패킷 인젝션 공격이 가능함을 보였다[4]. 이외에도 Vilches et al.(2018)은

로봇 시스템 보안 평가를 위한 표준화 프레임워크인 Robot Security Framework(RSF)를 제안하였고[6], Lera et al.(2016)은 ROS 기반 시스템의 보안 강화(hardening) 기법 성능을 실험적으로 평가하였다[7]. McClean et al.(2013)은 ROS의 사이버-물리 보안 취약성을 초기 단계에서 분석하였으며[8], Lacava et al.(2021)은 로봇 시스템의 사이버보안 이슈와 향후 연구 방향을 종합적으로 정리하였다[9].

그러나 기존 연구들은 주로 TLS 1.3 기반 전송 보안, 접근 제어, 펌웨어 무결성 검증 등 전통적 보안 기법에 집중되어 있으며[5], 양자컴퓨팅 환경에서의 선제적 보안 전환 필요성은 상대적으로 충분히 논의되지 못하였다. 특히 HNDL 공격 가능성을 고려할 때, 장기간 저장되는 인간 행동 데이터와 로봇 제어 데이터의 기밀성을 보호하기 위한 양자내성암호(PQC) 기반 보안 체계의 필요성이 점차 증가하고 있다.

2.2 양자컴퓨팅 위협의 최신 동향

양자컴퓨팅 기술은 최근 수년간 급격한 발전을 거듭하며 기존 공개키 암호 체계에 대한 실질적 위협으로 부상하고 있다. IBM은 2023년 1,121큐비트 규모의 Condor 프로세서를 발표하였으며, 향후 100,000큐비트급 시스템 구현을 목표로 하는 로드맵을 공개하였다[24]. Google Quantum AI는 2023년 surface code 기반 논리 큐비트의 오류율을 물리 큐비트 대비 절반 이하로 감소시키는 성과를 발표하여 fault-tolerant 양자컴퓨팅 실현 가능성을 높였다[25]. 이러한 기술 진보는 Mosca(2018)가 제시한 CRQC(Cryptographically Relevant Quantum Computer) 출현 가능성을 앞당길 수 있다는 우려를 낳고 있다[14].

국제 규제 기관들도 이에 대한 대응을 본격화하고 있다. 미국 NSA는 2022년 CNSA 2.0 지침을 발표하며 2030년까지 국가 안보 시스템에 대한 PQC 전환 계획을 제시하였고, EU의 ENISA는 2023년 보고서를 통해 장기 기밀성이 요구되는 통신 시스템에서의 선제적 PQC 전환 필요성을 강조하였다[26]. 이러한 국제적 동향은 인간 행동 데이터를 장기간 저장·전송하는 휴머노이드 시스템에서도 PQC 적용 필요성이 점차 현실화되고 있음을 시사한다.

국내에서도 제도적 대응이 본격화되고 있다. 특히 2026년 5월 개정된 「양자과학기술법」은 공공 인프라 보안 강화를 법적 의무화하고 있다. 이는 본 연구의 아키텍처가 국가 정책이 지향하는 '보안 필수 AI 융합 서비스' 범주에 포함됨을 시사하며 기술적 정당성을 부여한다[29].

2.3 상업용 휴머노이드 및 Physical AI의 최신 동향

휴머노이드 로봇 시장은 2023년 이후 빠른 성장세를 보이고 있다. Tesla의 Optimus Gen-2, Figure AI의 Figure 01, 1X Technologies의 NEO 등 다양한 상업용 플랫폼이 공개되었으며[27], 이들은 공통적으로 온보드 연산 한계를 보완하기 위한 클라우드 AI 연동 구조를 채택하고 있다. 특히 Figure AI는 2024년 OpenAI와의 협력을 통해 LLM 기반 실시간 대화 및 행동 계획 시스템을 시연한 바 있으며, 이는 로봇–클라우드 간 고대역폭·실시간 보안 통신의 중요성을 보여준 사례로 평가된다[27].

한편 EMS(Electrical Muscle Stimulation) 기반 인체 인터페이스와 연계되는 conceptual Physical AI 시스템도 개념적 수준에서 시연되고 있다[28]. 비록 해당 사례들은 peer-reviewed 연구 결과가 아닌 초기 단계의 개념적 시연 수준에 해당하지만, 클라우드-단말 간 통신 침해가 물리적 안전 문제로 이어질 수 있다는 보안 패러다임 전환 가능성을 시사하는 보조 사례로 참고할 수 있다[5].

2.4 기존 연구와의 차별성

〈Table 1〉은 기존 로봇 보안 연구와 본 연구의 차별점을 비교한 것이다. Quarta et al.(2017)과 Cheng et al.(2022)은 Intel x86 환경에서 RSA/ECC 및 TLS 수준의 보안을 다루나 양자 위협 대응은 포함하지 않으며, Kannwischer et al.(2019)은 ARM Cortex-M4에서 Kyber를 실측한 선도적 연구이나 MCU 환경에 국한되

〈Table 1〉 Comparison with Prior Studies

Study	Target Platform	PQC Adoption	Data-Type-Aware Analysis	Real-Time Guarantee
Quarta et al. (2017)	Intel x86	RSA/ECC	-	-
Cheng et al. (2022)	Intel x86	TLS	-	-
Kannwischer et al. (2019)	ARM Cortex-M4	Kyber	-	-
Open Quantum Safe (2024)	ARM / x86	ML-KEM	-	Partial
This Study	ARM Cortex-A72 (Literature-informed Estimate)	ML-KEM	3-data Modalities	Latency Bound Analysis

어 데이터 유형별 분석이나 실시간 보장은 다루지 않는다[3,4,16]. 본 연구는 ARM Cortex-A72 클래스 환경에 대한 literature-informed estimate를 기반으로 ML-KEM 적용 가능성을 분석하고, 음성·이미지·LiDAR 세 가지 모달리티에 대한 worst-case latency bound를 제시한다는 점에서 기존 연구와 차별화된다[18].

2.5 Post-Quantum Cryptography 표준화 동향

Shor(1994)의 알고리즘은 양자 컴퓨터를 이용하여 정수 인수분해 및 이산 로그 문제를 다항 시간 내 해결할 수 있음을 보임으로써, RSA 및 ECC 기반 공개키 암호 체계의 근본적 취약성을 제시하였다[11]. 또한 Grover(1996)의 알고리즘은 대칭키 암호의 유효 키 길이를 절반 수준으로 감소시키므로, 장기 보안성 확보를 위해 AES-256과 같은 고강도 대칭키 암호 적용 필요성이 제기되고 있다[12]. Mosca(2018)는 암호학적으로 유의미한 양자 컴퓨터(CRQC)가 향후 15년 내 등장할 가능성을 제시하며 선제적 대응의 필요성을 강조하였다[14]. 이에 따라 NIST는 2016년부터 PQC 표준화 공모를 진행하였으며, 격자 기반(Lattice-based), 해시 기반(Hash-based), 코드 기반(Code-based) 암호 체계를 평가한 끝에 2024년 최종 표준(FIPS 203~205)을 발표하였다[10]. 표준화 이전에도 격자 기반 키 교환 프로토콜에 대한 실용적 구현 연구가 활발히 수행되었으며, Bos et al.(2016)의 Frodo는 링 구조 없이 표준 LWE를 기반으로 한 실용적 키 교환 방식을 제안하였다[23]. ML-KEM는 Module Learning With Errors(MLWE) 문제의 계산적 난해성에 기반하며, 키 생성·캡슐화·복호화 과정에서 NTT(Number Theoretic Transform) 기반 다항식 연산을 활용한다[13]. LWE 문제의 구체적 난해성 수준에 대한 분석은 Albrecht et al.(2015)에 의해 체계적으로 정리되었다[17]. 또한 국내에서도 공공 부문 PQC 전환 정책 논의가 본격화되면서 국가 차원의 양자보안 체계 전환 필요성이 점차 확대되고 있다[21,29].

2.6 임베디드 환경에서의 PQC 성능

Kannwischer et al.(2019)의 pqm4 프로젝트는 ARM Cortex-M4 기반에서 다양한 PQC 후보군의 성능을 체계적으로 벤치마킹하였으며, Kyber512의 키 교환이 약 1.5ms 수준에서 수행 가능함을 보고하였다[16]. Open Quantum Safe Project(2024)는 ARM 및 x86 플랫폼에 걸친 포괄적 ML-KEM 성능 벤치마크를 제공하였다[18]. Fritzmann et al.(2020)은 RISC-V 기반 하드웨어 가속기를 활용하여 격자 기반 암호 연산을 수십 배 수준으로 가속할 수 있음을 보여주었다[19].

그러나 기존 연구들은 주로 마이크로컨트롤러(MCU) 또는 범용 서버 환경 중심으로 수행되었으며, 휴머노이드 로봇의 실제 운용 환경에 가까운 ARM Cortex-A 계열 SoC(NVIDIA Jetson, Raspberry Pi 등)에서 데이터 유형별 암호화 지연을 분석한 연구는 상대적으로 제한적이다[16]. 이에 본 연구는 해당 연구 공백에 대한 초기 단계의 탐색적 적용 가능성 분석을 수행하는 것을 목표로 한다.

3. ML-KEM 휴머노이드 적용 이론 분석

3.1 RSA와 ML-KEM 연산 복잡도 비교

RSA의 핵심 연산은 모듈러 지수승(Modular Exponentiation)으로, n비트 정수에 대해 $O(n^3)$의 계산 복잡도를 가지며 〈Table 2〉와 같이 비교 정리 하였다.

〈Table 2〉 Comparison of RSA-2048 and ML-KEM

Item	RSA-2048	ML-KEM-768
Core Mathematical Problem	Integer Factorization Problem (IFP)	Module Learning With Errors (Module-LWE / MLWE)
Core Operation	Modular exponentiation	NTT-based polynomial multiplication
Computational Complexity	$O(n^3)$	O(n log n)
Key Generation Workload	~10^9 operations	~10^4 operations
Memory Requirement	High (large-integer arithmetic)	Low (degree-256 polynomials)
Quantum Resistance	✗ (vulnerable to Shor's algorithm)	✓ (NIST FIPS 203)
Hardware Acceleration Suitability	Low	High (NTT-dedicated accelerators)

NTT(Number Theoretic Transform)는 이산 푸리에 변환(DFT)의 정수 체계 버전으로, 다항식 곱셈을 $O(n^2)$에서 O(n log n)으로 가속한다[21]. ML-KEM은 소수 q=3329, 차수 n=256인 다항식 환 $R_q = Z_q[x]/(x^{256}+1)$ 위에서 동작하며, NTT 도메인에서의 곱셈은 단순한 계수별(coefficient-wise) 곱셈으로 변환된다[13].

3.2 ARM 아키텍처에서의 ML-KEM 적합성

ARM Cortex-A 계열 프로세서는 SIMD(Single Instruction Multiple Data) 명령어 집합인 NEON을 지원하며, 이는 NTT 연산의 병렬화에 직접 활용될 수 있다[20]. 구체적으로 ARM NEON은 128비트 레지스터를 통해 16개의 8비트 또는 8개의 16비트 정수를 동시에 처리할 수 있어, ML-KEM의 계수별 연산을 효율적으로 가속한다[16]. 반면 RSA의 모듈러 지수승 연산은 수천 비트 정수에 대한 Barrett Reduction 또는 Montgomery Multiplication을 반복적으로 수행해야 하며, 이는 ARM Cortex-A의 32/64비트 정수 ALU 구조상 병렬화 효율이 낮다[20]. 재구성 가능 하드웨어(FPGA) 기반의 격자 암호 공개키 암호화 구현 연구도 이러한 가속 가능성을 뒷받침한다[22]. 결과적으로 ML-KEM은 ARM 기반 온보드 컴퓨팅 환경에서 RSA 대비 약 7.6배 빠른 키 교환을 실현하며, 이는 실시간 로봇 통신의 요구사항을 충족하는 핵심 근거가 된다[16,18].

〈Table 3〉 Literature-Informed Performance Estimates for ARM Cortex-A72 (Extrapolated)

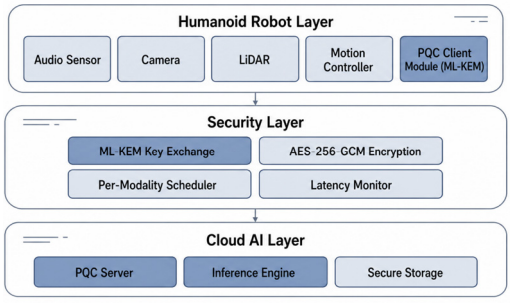
Algorithm	Key Generation (ms)	Encapsulation (ms)	Decapsulation (ms)	Total (ms)	Post-Quantum Secure
RSA-2048	8.4	0.3	8.1	~16.8	✗
ECDH-256	1.2	0.6	0.6	~2.4	✗
ML-KEM-512	0.4	0.5	0.4	~1.3	✓
ML-KEM-768	0.7	0.8	0.7	~2.2	✓
ML-KEM-1024	1.1	1.2	1.1	~3.4	✓

〈Table 3〉에 제시된 값들은 ARM Cortex-A72급 하드웨어를 대상으로 한 문헌 기반 스케일 추정치이며, Open Quantum Safe 벤치마크와 기존 임베디드 PQC 문헌을 바탕으로 도출된 것으로, 직접 재현한 측정 결과는 아니다[18].

4. 아키텍처 제안

4.1 시스템 구조 개요

본 연구에서 제안하는 PQC 기반 휴머노이드-클라우드 보안 아키텍처는 ① 휴머노이드 레이어, ② 보안 레이어, ③ 클라우드 AI 레이어의 3계층으로 구성하였으며 [Fig. 1]와 같다.

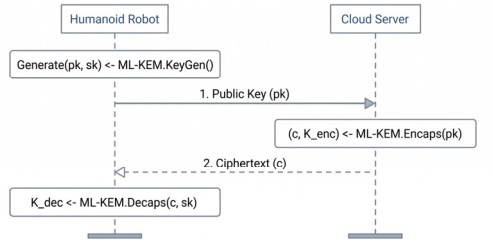


[Fig. 1] Proposed Three-Layer Architecture

각 계층은 독립적 보안 경계를 유지하며, 보안 레이어에서 ML-KEM 세션 키 교환과 AES-GCM 데이터 암호화를 중재한다.

4.2 ML-KEM 기반 세션 키 교환

ML-KEM-768 기반 세션 키 교환은 다음 [Fig. 2]와 같이 세 단계로 이루어진다[10,13]. 본 프로토콜은 서버 공개키(pk)에 대한 ML-DSA 서명 검증 또는 PKI 기반 인증과 결합되어 운용되며, 인증 실패 시 키 교환을 중단한다.



[Fig. 2] ML-KEM Key Exchange Protocol

4.3 데이터 유형별 하이브리드 암호화

휴머노이드 로봇이 생성하는 센서 데이터는 유형에 따라 크기와 실시간성 요구 수준이 크게 다르다. 본 연구는 세 가지 주요 데이터 유형을 정의하고, 각각에 대해 AES-256-GCM 기반 암호화를 적용한다. 휴머노이드 환경에서 생성되는 데이터는 음성(Audio), 영상(Image), LiDAR Point Cloud 등 서로 다른 모달리티 특성을 가지며, 각 데이터 유형은 요구되는 실시간성과 허용 가능

한 지연 범위가 상이하다. 일반적으로 음성 데이터는 약 10 KB/frame 수준의 비교적 작은 크기를 가지나 30~60 fps 수준의 높은 생성 주기를 가지므로 매우 낮은 지연 시간이 요구된다. 반면 영상 데이터는 약 1 MB/frame 규모로 대역폭 요구가 증가하며, LiDAR Point Cloud 데이터는 약 10 MB/frame 수준의 대용량 데이터를 포함하므로 상대적으로 높은 허용 지연 범위를 가진다. 본 연구에서는 이러한 모달리티별 특성을 고려하여 AES-256-GCM 기반 프레임 단위 암호화 구조를 적용하였다. 세션 키를 고정한 상태에서 프레임별 독립 nonce를 적용하여 암호화를 수행하였다. 또한 암호화 수행 시간을 측정하여 데이터 유형별로 정의된 latency bound를 초과하는 경우 실시간 보장 위반 상황으로 판단하도록 설계하였다. 최종적으로 암호문(ciphertext), 인증 태그(authentication tag), nonce 및 modality identifier를 함께 클라우드로 전송하는 구조를 적용하였다.

4.4 위협모델

본 연구는 Cyber-Physical AI 환경의 특수성을 반영하여 다섯 가지 공격 시나리오를 위협 모델로 〈Table 4〉와 같이 정의하였다. 특히 Physical AI 환경에서는 통신 침해가 물리적 결과로 직결될 수 있음을 강조한다

〈Table 4〉 Threat Scenarios

Attack Type	Potential Physical Impact	PQC Countermeasure
MITM	High Severity — actuator malfunction and unintended physical behavior	ML-KEM&ML-DSA authenticated key exchange
HNDL	Critical Severity — long-term exposure of behavioral data	PQC-based confidentiality protection
Replay Attack	Medium Severity — repeated or unintended actions	Per-frame nonce (replay mitigation)
Session Hijacking	High Severity — sustained abnormal operation	Authenticated session key renewal (ML-KEM + ML-DSA)
Actuator Command Tampering	Critical Severity — direct physical manipulation risk	AES-256-GCM authentication tag verification

MITM 공격에 대해 ML-KEM 기반 키 교환은 공개키 위변조를 ML-DSA 서명 검증으로 차단하여 인증된 상대방과의 세션만 성립되도록 보장한다. HNDL 위협에 대해서는 PQC 기반 키 교환을 통해 현재 암호화된 트래픽이 미래의 양자 컴퓨터로도 복호화될 수 없도록 장기 기밀성을 확보한다. Replay Attack은 프레임별 독립 nonce 적용으로 동일 암호문의 재전송을 무효화한다. Session Hijacking은 ML-KEM과 ML-DSA 기반의 인증된 세션 갱신 구조를 통해 세션 탈취 후 지속적 악용을 방지한다. Actuator Command Tampering은 AES-256-GCM의 128비트 인증 태그 검증을 통해 명령 변조 시 즉시 거부되도록 설계하였다.

4.5 AES-256-GCM 선택 근거

본 연구에서는 대용량 센서 데이터 암호화를 위한 대칭키 알고리즘으로 AES-256-GCM을 적용하였다. 해당 알고리즘을 선택한 주요 근거는 다음과 같다. 첫째, AES-GCM은 Authenticated Encryption with Associated Data(AEAD) 구조를 기반으로 기밀성(confidentiality)과 무결성(integrity)을 단일 패스(single-pass)에서 동시에 제공하며, 128비트 인증 태그(authentication tag)를 통해 데이터 변조 여부를 효과적으로 검증할 수 있다[10]. 둘째, CTR(Counter) 모드 기반의 스트림 암호화 구조를 사용하므로 패딩(padding)이 필요하지 않으며, CBC 계열 모드 대비 병렬 처리에 유리하여 낮은 연산 오버헤드를 제공한다. 셋째, ARMv8 cryptographic extensions와 같은 하드웨어 암호화 가속 기능을 활용할 경우 임베디드 환경에서도 높은 처리량을 확보할 수 있어 실시간 센서 데이터 암호화에 적합하다[20]. 넷째, 프레임별 독립적인 96비트 nonce를 적용함으로써 Replay Attack에 대한 방어 기능을 제공할 수 있다. 다섯째, AES-256은 Grover 알고리즘 적용 환경에서도 약 128비트 수준의 유효 보안 강도를 유지할 수 있어 양자 컴퓨팅 환경에서도 상대적으로 높은 장기 보안성을 제공한다[12].

5. 성능평가

5.1 성능평가 환경

본 연구는 두 가지 성능평가 환경을 기반으로 성능을 분석하였다. 우선 Intel Core i7-12700 기반 PC 환경에서 AES-256-GCM 및 ML-KEM 연산의 기준 성능을 실측하였다. 이후 ARM Cortex-A72 기반 임베디드 환경에 대해서는 Raspberry Pi 4 수준의 성능 특성을 가정하고, 선행 ARM PQC 벤치마크 문헌과 liboqs 공식 성능 평가 결과를 기반으로 literature-informed extrapolated

estimate를 적용하였으며 환경구성은 〈Table 5〉와 같다[16,18].

〈Table 5〉 Benchmark Configuration

Category	PC Baseline Environment	ARM Extrapolated Estimate
Platform	Intel Core i7-12700	ARM Cortex-A72 (RPi 4 equivalent)
PQC Library	liboqs 0.15.0	liboqs 0.10.x (ARM build assumption)
Evaluation Method	Direct measurement	Literature-informed extrapolation

PQC 구현은 liboqs 0.15.0 라이브러리를 사용하여 본 연구 실험 환경(Intel Core i7-12700, Windows 11)에서 직접 실측하였다. ML-KEM-768 기준 KeyGen 0.1353ms, Encaps 0.1572ms, Decaps 0.1916ms, 합산 0.4841ms로 측정되었다. ARM 환경 추정치는 x86-64 대비 ARM Cortex-A72의 PQC 성능 비율이 문헌상 약 2.5~3.5배로 보고된 점을 토대로 보수적 상한값 ×4.0을 적용하여 산출하였으며, 실제 Jetson 또는 Raspberry Pi 환경에서 직접 측정된 값이 아닌 탐색적 적용 가능성 분석임을 전제로 한다.

5.2 프로토타입 구현 환경 및 측정 방법

본 연구의 프로토타입 구현 및 성능평가 실험은 Python 3.14 환경에서 cryptography 46.x 라이브러리를 활용하여 수행하였다. AES-256-GCM 암호화는 AESGCM 클래스를 기반으로 구현하였으며, 키 교환 성능 비교를 위해 X25519 ECDH 및 RSA-2048 연산 성능을 함께 측정하였다. ML-KEM-768의 연산 지연은 본 연구의 아키텍처 수준 적용 가능성 분석 목적에 부합하도록 Open Quantum Safe Project 벤치마크[18] 및 선행 임베디드 PQC 문헌[16]을 인용한 literature-informed estimate로 제시하였으며, 실측 검증은 후속 연구로 위임한다. 측정 신뢰도 확보를 위해 초기 warm-up 10회를 제외한 후 총 1,000회의 반복 측정을 수행하였으며, 평균(mean), 중앙값(median), 표준편차(standard deviation), 백분위수(p95, p99), worst-case latency를 주요 통계량으로 산출하였다. 또한 멀티스레드 동시 암호화 실험(Experiment 3)에서는 threading.Barrier를 활용하여 세 개의 모달리티 스레드가 동시에 시작되도록 구성하였다. 30fps 스트림 환경을 가정한 Experiment 4에서는 연속 프레임 처리 과정에서 33.33ms latency budget 초과 여부를 기준으로 실시간 요구사항 충족 가능성을 평가하였다. 성능 평가는 평균 latency(mean latency), 백분위수 지연(p95/p99), worst-case latency, throughput(MB/s), CPU usage 등을 기준으로 수행하였다. nonce는 매 프레임 os.urandom(12)를 통해 96비트 난수로 생성하였으며, 모달리티별 테스트 데이터는 os.urandom() 기반 의사난수 바이트열로 생성하였다. CPU 사용률은 Python psutil 라이브러리의 cpu_percent() 함수를 암호화 연산 전후로 호출하여 측정하였다. 또한 ARM 기반 임베디드 환경 적용 가능성 평가는 기존 PC 측정값에 문헌 기반 ARM scaling factor를 적용하여 추정하였다. 다만 본 결과는 실제 Jetson 또는 Raspberry Pi 환경에서 직접 측정된 값이 아니라, 선행 문헌 기반의 exploratory feasibility estimate임을 전제로 한다.

5.3 성능평가 결과 분석

5.3.1 PC기반 성능평가 결과

우선 Intel Core i7-12700 기반 PC 환경에서 AES-256-GCM 암호화 성능에 대한 성능평가를 수행하였다. 실험은 Audio(10 KB), Image(1 MB), LiDAR Point Cloud(10 MB)의 세 가지 데이터 모달리티를 대상으로 수행되었으며, 총 1,000회의 반복 측정을 통해 평균 latency, p95/p99 latency, worst-case latency 및 처리량을 분석하였다. 측정 결과, 모든 데이터 유형에서 AES-256-GCM 암호화 지연은 실시간 요구사항(latency budget)을 충분히 만족하는 것으로 나타났다. 특히 Audio 데이터의 평균 암호화 지연은 0.0026ms 수준으로 측정되었으며, LiDAR 데이터 역시 평균 3.78ms 수준으로 50ms 허용 지연 범위 이내를 안정적으로 유지

〈Table 6〉 PC Benchmark Results

Data Type	Size	Mean (ms)	p95 (ms)	p99 (ms)	Worst (ms)	Stdev	Throughput (MB/s)	CPU Usage (%)	Latency Budget	Result
Audio	10 KB	0.0026	0.0026	0.0051	0.046	0.0016	3,756	0.0*	〈 5 ms	✓
Image	1 MB	0.3736	0.4584	0.5921	0.9051	0.0502	2,677	48.4	〈 20 ms	✓
LiDAR	10 MB	3.7772	4.1481	4.4453	5.1315	0.1952	2,648	81.7	〈 50 ms	✓

하였다. 또한 Image 데이터 기준 AES 처리량은 약 2,677 MB/s 수준으로 측정되어, PC 환경에서는 대용량 멀티모달 센서 데이터에 대해서도 실시간 암호화 처리가 가능함을 시사하며 결과는 〈Table 6〉와 같다.

5.3.2 ARM Cortex-A72 기반 적용 가능성 분석

휴머노이드 로봇의 실제 운용 환경은 NVIDIA Jetson 및 Raspberry Pi 계열과 같은 ARM Cortex-A 기반 임베디드 플랫폼이 주로 사용된다. 이에 본 연구에서는 PC 기반 성능평가 결과를 기반으로 ARM 환경에서의 적용 가능성을 분석하기 위해 문헌 기반 분석을 수행하였다. ARM 추정치는 x86-64와 ARM Cortex-A 간 PQC 성능 비율이 문헌상 약 2.5~3.5배로 보고된 점[16,18]을 토대로, 보수적 상한값 ×4.0을 적용하여 산출하였다. Cortex-A72의 NEON SIMD 활용 시 실제 비율은 이보다 낮을 수 있다.

분석 결과, ARM Cortex-A72 수준의 환경에서도 AES-256-GCM 암호화 지연은 모든 데이터 모달리티에서 실시간 요구사항을 만족할 가능성을 보였다. Audio 데이터의 평균 추정 latency는 약 0.010ms 수준으로 나타났으며, LiDAR 데이터 역시 worst-case 기준 약 20.5ms 수준으로 50ms latency budget 이내를 유지하는 것으로 분석되었으며 〈Table 7〉과 같다.

이는 ARM 기반 임베디드 환경에서도 PQC 기반 보안 구조와 AES-256-GCM 암호화가 실시간 휴머노이드 통신 요구사항과 병행 가능함을 시사한다.

〈Table 7〉 Latency Estimates for AES-256-GCM on ARM Cortex-A72 (Applying ×4.0 Scaling Factor)

Data Type	Mean Estimate (ms)	p99 Estimate (ms)	Worst Estimate (ms)	Latency Budget (ms)	Result
Audio (10 KB)	0.01	0.02	0.184	5	✓
Image (1 MB)	1.494	2.368	3.620	20	✓
LiDAR (10 MB)	15.109	17.781	20.526	50	✓

다만 본 결과는 실제 Jetson 또는 Raspberry Pi 환경에서 직접 측정된 값이 아니라, 선행 임베디드 PQC 성능평가 문헌을 기반으로 수행된 초기 단계의 탐색적 적용 가능성 분석임을 전제로 한다. 또한 ×4.0 scaling factor는 정확한 하드웨어 등가 모델이라기보다, 선행 ARM 성능평가 결과를 기반으로 한 보수적 근사값으로 해석되어야 한다. 따라서 본 결과는 실제 임베디드 배포 환경에서 직접 검증된 실측 결과라기보다, 문헌 기반의 적용 가능성 추정 결과로 이해되어야 한다.

5.3.3 실시간 스트림 성능 분석

30fps 환경에서는 프레임당 약 33.33ms 이내에서 암호화 및 전송 처리가 완료되어야 실시간성이 유지될 수 있다. 이에 본 연구에서는 30fps 기준 10초(300프레임) 연속 스트림 환경을 가정하여, AES-256-GCM 암호화 과정에서 latency budget 초과 여부(deadline miss)를 측정하였다. 또한 기존 30프레임(1초) 수준의 단기 측정보다 측정 구간을 확장함으로써, tail latency 및 sporadic spike 발생 여부를 보다 안정적으로 관찰하고자 하였다.

분석 결과는 〈Table 8〉과 같으며, 300프레임(30fps × 10초) 연속 스트림 환경에서 모든 데이터 유형에 대해 deadline miss는 발생하지 않았다(0/300). 특히 LiDAR 데이터의 경우 worst-case latency가 약 5.27ms 수준으로 측정되어, 33.33ms frame budget 대비 충분한 여유를 유지하는 것으로 나타났다.

〈Table 8〉 30fps Real-Time Stream Profiling Results

Data Type	Mean (ms)	Worst (ms)	Frame Budget (ms)	Deadline Miss	Miss Rate
Audio (10 KB)	0.0035	0.3274	33.33	0/300	0.00%
Image (1 MB)	0.3938	1.4239	33.33	0/300	0.00%
LiDAR (10 MB)	3.8043	5.2689	33.33	0/300	0.00%

이는 PC baseline 환경에서 AES-256-GCM 암호화 지연과 ML-KEM-768 키 교환 지연(실측: 0.4841ms)을 합산하더라도 모든 데이터 유형에서 실시간 latency budget 이내임을 동일 환경 실측값으로 확인한 결과이며, 10초 연속 측정 환경에서도 tail latency 안정성이 유지됨을 보여준다. 멀티모달 데이터 동시 처리 환경에서도 실시간 latency budget을 안정적으로 만족하였다.

5.3.4 키 교환 성능 비교

PC기반 환경에서 X25519 ECDH와 RSA-2048의 키 교환 성능을 비교하였으며, ML-KEM-768의 경우 선행 문헌 기반 추정값을 함께 제시하였다. RSA-2048 key generation latency는 총 30회 반복 측정을 통해 산출

하였고, X25519 ECDH 및 AES benchmark는 warm-up 10회를 제외한 후 1,000회 반복 측정을 수행하였다. ML-KEM-768 관련 수치는 Open Quantum Safe Project 및 선행 PQC benchmark 문헌 기반의 literature-informed estimate를 적용하였다[18].

〈Table 9〉 Key Exchange Performance Comparison

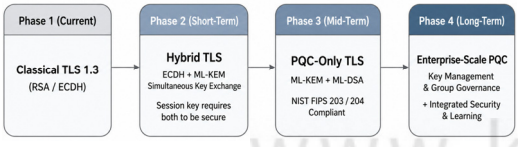
Metric	RSA-2048	X25519 ECDH	ML-KEM-768 (Estimated)
Mean Key Exchange Latency (ms)	35.53	0.1	~0.5
Worst-Case Latency (ms)	129.49	1.15	~2.2 (ARM)
p95 Latency (ms)	~127.8	~0.08	—
Public Key Size (bytes)	256	32	1,184
Ciphertext Size (bytes)	256	32	1,088
Quantum Resistance	✗	✗	✓ NIST FIPS 203

분석 결과는 〈Table 9〉와 같으며, RSA-2048의 평균 key generation latency는 약 35ms 수준으로 측정되었으며, worst-case latency는 약 129ms에 도달하였다. 반면 X25519 ECDH는 평균 약 0.10ms 수준으로 측정되어 RSA-2048 대비 매우 낮은 지연 특성을 보였다. 또한 문헌 기반 추정에 따르면 ML-KEM-768은 PC 환경에서 약 0.5ms, ARM Cortex-A72 환경에서는 약 2.2ms 수준의 latency를 보일 것으로 예상되며, 이는 실시간 휴머노이드 통신 환경에서도 적용 가능성을 가질 수 있음을 시사한다.

6. 결론

6.1 Hybrid PQC Migration 전략

현실적인 배포 환경에서 기존 TLS 인프라를 즉시 PQC 기반 구조로 전환하는 것은 상호운용성(interoperability) 및 기존 시스템 호환성 문제로 인해 쉽지 않다. 이에 본 연구는 기존 TLS 1.3 환경과의 호환성을 유지하면서 단계적으로 PQC를 도입할 수 있는 Hybrid PQC Migration 전략을 [Fig. 3] 와 같이 제안한다[15].



[Fig. 3] Hybrid PQC Migration Framework

초기 단계(Phase 1)에서는 기존 RSA/ECDH 기반 Classical TLS 1.3 구조를 유지한다. 이후 단기 단계(Phase 2)에서는 ECDH와 ML-KEM을 동시에 사용하는 Hybrid TLS 구조를 적용하여, 기존 공개키 기반 보안성과 양자내성 기반 보안성을 병렬적으로 확보한다. 해당 방식은 양측 키 교환 결과가 모두 유효할 경우에만 최종 세션 키가 생성되는 구조를 가정한다. 중기 단계(Phase 3)에서는 ML-KEM 및 ML-DSA 기반의 PQC-only TLS 환경으로 점진적으로 전환하며, NIST FIPS 203/204 표준 준수를 목표로 한다. 마지막 장기 단계(Phase 4)에서는 다중 로봇 환경에서의 PQC 기반 그룹 키 관리와 Federated Learning 보안 통합 구조로 확장될 수 있다.

특히 Phase 2의 Hybrid TLS 접근은 최근 IETF RFC 초안에서도 논의되고 있으며, 기존 TLS 1.3 핸드셰이크 구조를 유지하면서 ML-KEM ciphertext를 추가 키 공유 요소로 결합하는 방식으로 구현될 수 있다[15]. 이러한 접근은 양자컴퓨터가 실질적 위협으로 현실화되기 이전 단계에서도 HNDL(Harvest-Now, Decrypt-Later) 공격에 대한 선제적 대응 가능성을 제공하며, 동시에 기존 인프라와의 하위 호환성을 유지할 수 있다는 장점을 가진다.

6.2 연구의 한계 및 향후 검증 방향

본 연구는 휴머노이드-클라우드 통신 환경에서의 PQC 적용 가능성을 architecture 수준에서 분석한 preliminary feasibility-oriented investigation의 성격을 가지며, 다음과 같은 한계를 지닌다. 이러한 한계는 향후 실증 연구를 통해 추가적으로 검증될 필요가 있다.

첫째, 본 연구는 NVIDIA Jetson 또는 Raspberry Pi 4와 같은 실제 ARM 기반 임베디드 플랫폼에 직접 배포하여 측정한 결과가 아니라, 선행 임베디드 PQC benchmark 문헌을 기반으로 한 literature-informed estimate를 활용하였다. 따라서 향후 연구에서는 Jetson Orin NX 등 실제 ARM 기반 플랫폼 환경에서의 실측 검증이 필요하다.

둘째, ARM 환경 추정 과정에서 PC baseline 결과에 보수적 scaling factor(×4.0)를 적용하였으나, 실제 환경에서는 캐시 구조, 메모리 대역폭, 하드웨어 가속 여부 등에 따라 성능 차이가 발생할 수 있다. 이에 따라 실제 ARM 플랫폼 기반 benchmark를 통한 scaling factor 보정이 요구된다.

셋째, 본 연구는 암호화 및 키 교환 과정의 연산

latency를 중심으로 분석하였으며, 실제 WiFi·5G 기반 네트워크 환경에서 발생할 수 있는 패킷 손실(packet loss), 네트워크 지터(jitter), E2E(end-to-end) 지연 등은 포함하지 않았다. 향후 연구에서는 실제 무선 통신 환경을 고려한 통합 성능 검증이 필요하다.

넷째, 배터리 기반 휴머노이드 플랫폼에서 중요한 요소인 전력 소비 및 에너지 오버헤드에 대한 분석은 수행하지 않았다. 따라서 향후 전력 프로파일링(power profiling) 기반 에너지 효율 분석이 추가적으로 요구된다.

다섯째, 본 연구는 단일 로봇-클라우드 구조를 가정하였으며, 다중 로봇 환경에서 요구되는 PQC 기반 그룹 키 관리 및 Federated Learning 보안 구조는 다루지 않았다. 향후 연구에서는 multi-robot PQC group key protocol 및 분산 협업 환경에서의 PQC 기반 모델 업데이트 보호 구조로 확장될 필요가 있다.

마지막으로, 실제 ROS2 미들웨어 및 DDS(Data Distribution Service) 계층과의 통합 구조는 본 연구 범위에 포함하지 않았다. 따라서 향후 ROS2 DDS 레이어와의 PQC 통합 및 실시간성 영향 분석이 수행되어야 한다.

6.3 결론

본 연구는 휴머노이드-클라우드 통신 및 Physical AI 환경을 대상으로, ML-KEM-768기반 양자내성 키 교환과 AES-256-GCM 하이브리드 암호화를 결합한 PQC 보안 아키텍처의 필요성과 적용 가능성을 아키텍처 수준에서 분석하였다. 본 연구는 실제 임베디드 배포 환경에서 수행된 실증 연구가 아니라, 선행 임베디드 PQC 성능평가 문헌과 PC 기반 측정 결과를 기반으로 수행된 초기 단계의 탐색적 적용 가능성 분석 연구임을 전제로 한다.

본 연구의 주요 기여는 다음과 같이 요약될 수 있다. 첫째, MITM 기반 액추에이터 조작이 물리적 안전 위협으로 이어질 수 있는 가능성을 분석함으로써, Cyber-Physical AI 환경에서의 PQC 도입이 단순한 보안 기능 향상을 넘어 물리적 안전 보장을 위한 핵심 요구사항으로 고려될 필요가 있음을 제시하였다. 둘째, ML-KEM의 NTT 기반 연산 구조와 AES-256-GCM의 AEAD 특성을 결합하여, ARM 기반 임베디드 환경에서도 적용 가능한 경량 보안 아키텍처 방향성을 제안하였다. 셋째, Audio·Image·LiDAR 데이터에 대한 latency profiling과 ARM 기반 적용 가능성 분석을 통해, 실시간 휴머노이드 통신 환경에서의 적용 가능성을 예비 수준에서 분석하였다. 넷째, 기존 TLS 인프라와의 상호운용성을 고려한 단계적 Hybrid PQC Migration 전략을 제안하고, 향후 실증 연구를 위한 검증 방향과 한계를 함께 제시하였다.

휴머노이드 및 Cyber-Physical AI 시스템이 인간과 지속적으로 상호작용하는 Cyber-Physical 인프라로 확장됨에 따라, 클라우드-로봇 간 통신 보안은 단순한 데이터 기밀성 보호를 넘어 물리적 안전 보장의 문제로 확장되고 있다. 특히 HNDL 공격의 장기적 위협을 고려할 때, 인간 행동 데이터를 지속적으로 저장·전송하는 시스템에서는 PQC 기반 보안 전환에 대한 선제적 검토가 필요할 수 있다.

향후 연구에서는 NVIDIA Jetson Orin NX 기반 실물 ARM 플랫폼 실측 검증, ROS2 미들웨어 통합, 다중 로봇 환경에서의 PQC 기반 그룹 키 관리, Federated Learning 환경에서의 PQC 기반 모델 보호 구조 등으로 연구 범위를 확장할 예정이다[18].

REFERENCES

[1] Boston Dynamics, Atlas Robot Technical Overview [Internet], https://www.bostondynamics.com/atlas.(Accessed: May 14, 2026)

[2] B.Kehoe, S.Patil, P.Abbeel and K.Goldberg, "A Survey of Research on Cloud Robotics and Automation," IEEE Transactions on Automation Science and Engineering, Vol.12, No.2, pp.398-409, 2015.

[3] D.Quarta, M.Pogliani, M.Polino, F.Maggi, A.M.Zanchettin and S.Zanero, "An Experimental Security Analysis of an Industrial Robot Controller," in Proceedings of the 2017 IEEE Symposium on Security and Privacy, San Jose, 2017, pp.268-286.

[4] B.Dieber, R.White, S.Taurer, B.Breiling, G.Caiazza, H.Christensen and A.Cortesi, "Penetration Testing ROS," in Robot Operating System (ROS): The Complete Reference (Volume 4), A.Koubaa, Ed., Cham: Springer, Ch.6, pp.183-225, 2020.

[5] J.P.A.Yaacoub, H.N.Noura, O.Salman and A.Chehab, "Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations," International Journal of Information Security, Vol.21, No.1, pp.115-158, 2022.

[6] V.M.Vilches, E.Gil-Uriarte, V.Mayoral-Vilches, J.L.Hernández-Ramos and T.Sheridan, "Introducing the Robot Security Framework (RSF), a Standardized Methodology to Perform Security Assessments in Robotics," arXiv preprint arXiv:1806.04042, 2021 (v4). (Accessed: May 14, 2026)

[7] F.J.R.Lera, J.Balsa, F.Casado, C.Fernández, F.M.Rico and V.Matellán, "Cybersecurity in Autonomous Systems: Evaluating the Performance of Hardening ROS," in Proceedings of the Workshop on Security and Privacy in Robotics, IROS 2016, Daejeon, 2016.

[8] J.McClean, C.Stull, C.Farrar and D.Mascareñas, "A Preliminary Cyber-Physical Security Assessment of the Robot Operating System (ROS)," in Proceedings of SPIE Defense, Security, and Sensing, Baltimore, 2013, Vol.8741.

[9] G.Lacava, A.Marotta, F.Martinelli, A.Saracino, A.La Marra, E.Gil-Uriarte and V.M.Vilches, "Cybersecurity Issues in Robotics," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol.12, No.3, pp.1-28, 2021.

[10] National Institute of Standards and Technology, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard," U.S. Department of Commerce, 2024.

[11] P.W.Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, 1994, pp.124-134.

[12] L.K.Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in Proceedings of the 28th Annual ACM Symposium on Theory of Computing, Philadelphia, 1996, pp.212-219.

[13] R.Avanzi, J.Bos, L.Ducas, E.Kiltz, T.Lepoint, V.Lyubashevsky, J.M.Schanck, P.Schwabe, G.Seiler and D.Stehlé, "CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation," NIST PQC Round 3 Submission, 2021.

[14] M.Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," IEEE Security & Privacy, Vol.16, No.5, pp.38-41, 2018.

[15] C.Paquin and D.Stebila, "Post-Quantum TLS without Handshake Signatures," in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, 2020, pp.1461-1480.

[16] M.J.Kannwischer, J.Rijneveld, P.Schwabe and K.Stoffelen, "pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4," IACR ePrint Archive, Report 2019/844, 2019.

[17] M.R.Albrecht, R.Player and S.Scott, "On the Concrete Hardness of Learning with Errors," Journal of Mathematical Cryptology, Vol.9, No.3, pp.169-203, 2015.

[18] Open Quantum Safe Project, OQS-OpenSSL Performance Benchmarks on ARM and x86 Platforms[Internet], https://openquantumsafe.org/benchmarking.(Accessed: May 15, 2026)

[19] T.Fritzmann, G.Sigl and J.Sepúlveda, "RISQ-V: Tightly Coupled RISC-V Accelerators for Post-Quantum Cryptography," IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol.2020, No.4, pp.239-280, 2020.

[20] ARM Holdings, "Cortex-A72 Processor Technical Reference Manual," ARM Architecture Reference Manual, 2022.

[21] P.Longa and M.Naehrig, "Speeding Up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography," in Cryptology and Network Security - CANS 2016, Milan, 2016, pp.124-139.

[22] T.Pöppelmann and T.Güneysu, "Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware," in Selected Areas in Cryptography - SAC 2013, Burnaby, 2014, pp.68-85.

[23] J.Bos, C.Costello, L.Ducas, I.Mironov, M.Naehrig, V.Nikolaenko, A.Raghunathan and D.Stebila, "Frodo: Take Off the Ring! Practical, Quantum-Secure Key Exchange from LWE," in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Vienna, 2016, pp.1006-1018.

[24] IBM Research, "IBM Quantum System Two: The Era of Quantum Utility Is Here"[Internet], https://www.ibm.com/quantum/blog/quantum-roadmap-2033. (Accessed: May 14, 2026)

[25] Google Quantum AI, "Suppressing Quantum Errors by Scaling a Surface Code Logical Qubit," Nature, Vol.614, pp.676-681, 2023.

[26] National Security Agency, "Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)," NSA Cybersecurity Advisory, 2022.

[27] Figure, "Figure Raises $675M at $2.6B Valuation and Signs Collaboration Agreement with OpenAI" [Internet], PR Newswire, Feb. 29, 2024, https://www.prnewswire.com/news-releases/figure-raises-675m-at-2-6b-valuation-and-signs-collaboration-agreement-with-openai-302074897.html.(Accessed: May 14, 2026)

[28] P.He, A.Neall, V.Danry, D.Kaijzer, Y.Wu and S.Lewis, "Human Operator: AI-Guided Electrical Muscle Stimulation for Human Motor Augmentation," Hackathon Project, MIT Hard Mode 2026, MIT Media Lab, Cambridge, MA, 2026.

[29] Ministry of Science and ICT, "Partial Amendment Bill of the Act on the Promotion of Quantum Science and Technology and Quantum Industry Passed by the Cabinet," Policy Press Release, May 12, 2026.

장 상 현(Sang-hyun Jang) [정회원]

- 2012년 2월 : 세종사이버대학교 정보보호시스템학과 학사
- 2015년 8월 : 동국대학교 국제정보대학원 정보보호전공 석사
- 2023년 2월 : 숭실대학교 IT정책경영학과 공학박사
- 2026년 1월 ~ 현재 : 국가첨단백신개발센터 항원디자인팀장

〈관심분야〉
IT정책경영, 정보보호, 양자내성암호, 클라우드, AI

박 동 성(Dong-seong Park) [정회원]

- 2013년 2월 : 부산대학교 생명과학과/물리학과 학사
- 2022년 8월 : 안동대학교 백신공학과 석사
- 2024년 10월 ~ 현재 : 국가첨단백신개발센터 항원디자인팀

〈관심분야〉
백신, AI, 계산화학, 물리 시뮬레이션

김 동 주(Dongju Kim) [정회원]

- 1999년 2월 : 경북대학교 물리학과 이학사
- 2011년 2월 : 대구가톨릭대학교 컴퓨터정보통신공학과 공학석사
- 2021년 3월 ~ 현재 : 경북대학교 컴퓨터학부 공학박사수료
- 2020년 3월 ~ 현재 : 대구가톨릭대학교 컴퓨터소프트웨어학부 교수

〈관심분야〉
Game, AI, Mobile, IoT, Edge computing