사물인터넷융복합논문지 Vol. 12, No. 3, pp. 159-170, 2026 https://doi.org/10.20465/KIOTS.2026.12.3.159

원전 해체 핵종분석 데이터의 무결성 및 오류 추적을 위한 양자내성 기반 디지털 감사 아키텍처 설계 연구

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

Design of a Post-Quantum Cryptography-Based Digital Audit Architecture for Ensuring Integrity of Nuclide Analysis Data in Nuclear Decommissioning

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 원전 해체 과정에서 생성되는 핵종분석 데이터는 방사성폐기물 분류, 규제 기준 준수, 작업자 안전 프로토콜의 핵심 입력으로 기능한다. 2025년 6월 원안위의 고리 1호기 해체 승인과 2024년 12월 원복연 개원에 따라 데이터 무결성 보장은 현실적 운영 요건이 되었다. 그러나 기존 시스템은 단계별 오류 추적 및 전주기 무결성 보장 메커니즘이 부재하며 HNDL 공격에 취약하다. 본 연구는 NIST FIPS 203(ML-KEM-768) 및 FIPS 204(ML-DSA-65) 기반 양자내성 디지털 감사 아키텍처를 제안한다. 핵심 기여는 ① SHA-3 해시체인 기반 단계별 오류 추적, ② 원안위·KINS 연동 RDI 모델, ③ 12년 이상 장기 일정을 위한 암호 민첩성 설계, ④ 자연 변동과 의도적 조작을 구분하는 동적 임계값 알고리즘(DTA)이다. 6가지 공격 시나리오 실험에서 E3~E6 탐지율 100%·FP율 0.00%, E2 노이즈 시나리오에서 DTA 적용 후 FP율 100%→0.2% 감소를 확인하였으며, 경계 영역(±10%) 탐지율은 8.8%로 해시체인과의 병용 구조가 필요함을 실험적으로 확인하였다. PQC 처리 오버헤드는 배치 처리 주기 대비 0.001~0.015% 수준으로 나타났으며, 공개 핵종 데이터 및 감마선 스펙트럼 기반 시뮬레이션 환경에서 제안 아키텍처의 기술적 타당성과 적용 가능성을 예비적으로 확인하였다.

주제어 : 원전 해체, 핵종 분석, 양자내성암호, 데이터 무결성, 디지털 감사추적, ML-KEM, ML-DSA, 규제 안전성

Abstract Nuclide analysis data generated during nuclear decommissioning serves as critical input for radioactive waste classification, regulatory compliance, and worker safety. Following the NSSC's approval of Kori Unit 1 decommissioning in June 2025 and the establishment of the Korea Research Institute of Decommissioning (KRID) in December 2024, ensuring data integrity has become a practical operational requirement. Existing systems, however, lack step-by-step audit mechanisms and remain vulnerable to Harvest Now, Decrypt Later (HNDL) attacks. This study proposes a post-quantum cryptography (PQC)-based digital audit architecture grounded in NIST FIPS 203 (ML-KEM-768) and FIPS 204 (ML-DSA-65), incorporating four core contributions: ① a SHA-3 hash chain-based error tracing mechanism, ② a Regulatory Decision Integrity (RDI) model integrated with NSSC and KINS procedures, ③ a Crypto Agility strategy for decommissioning schedules exceeding 12 years, and ④ a Dynamic Threshold Algorithm (DTA) that distinguishes natural counting fluctuations from intentional manipulation. Experiments across six attack scenarios using IAEA nuclide datasets and ORNL gamma-ray spectra achieved 100% detection rates and 0.00% false positive rates for E3–E6, while DTA reduced the false positive rate from 100% to 0.2% in the E2 noise scenario, with a detection rate of 8.8% in the boundary region (±10%), confirming that a hybrid structure combining DTA with the hash chain is necessary. PQC processing overhead remained within 0.001–0.015% of the batch cycle, while the technical feasibility and applicability of the proposed architecture were preliminarily examined using public nuclide datasets and gamma-ray spectrum-based simulation environments.

Key Words : Nuclear decommissioning, nuclide analysis, post-quantum cryptography, data integrity, digital audit, ML-KEM, ML-DSA, regulatory safety

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

1. 서론

전 세계적으로 가동 연한이 만료된 원자력 발전소의 해체 프로젝트가 본격화되고 있다. 국제원자력기구(IAEA)의 보고에 따르면 2025년 기준 전 세계 209기의 원자로가 영구정지 상태에 있으며, 이 중 상당수가 해체 절차를 이행 중이거나 계획 단계에 있다[1]. 국내에서는 2025년 6월 26일 원자력안전위원회가 국내 최초 상업용 원전인 고리 1호기(가압경수로형, 595MWe)의 최종 해체계획서를 최종 승인하였다[3]. 2017년 영구정지 이후 8년 만의 승인으로, 한수원은 2025년 7월부터 터빈건물 내 설비 해체를 시작으로 2037년까지 총 1조 713억 원을 투입하여 단계적 해체 및 부지 복원을 추진한다[3].

제1 저자는 한국원자력환경공단(KORAD) 및 한국원자력환경복원연구원(이하 원복연) 재직 경험을 보유하고 있으며, 특히 원복연에서 원전 해체 관련 정보화 업무 전반을 담당하면서 핵종분석 데이터의 디지털 관리 체계와 그 구조적 취약점에 대한 실무적 문제의식을 도출하였다. 이에 본 연구는 단순한 기술적 제안이 아닌, 실제 운영 환경에 대한 현장 관찰에 기반한다.

2024년 12월에는 원복연이 부산 기장군에 개원하여 해체 폐기물의 방사능 핵종 분석 및 데이터베이스 구축 업무를 본격화하였다[6]. 원전 해체 과정에서 핵종분석은 방사성폐기물의 분류 기준 결정과 규제 기관 승인 획득을 위한 핵심 기술적 근거이다[2]. 특히 고순도 게르마늄(High-Purity Germanium, 이하 HPGe 검출기) 기반의 감마선 스펙트럼 데이터, 피크 핏팅 결과, 핵종별 방사능 활도(Activity) 값은 규제 의사결정의 직접적 입력이 되므로 그 정확성과 무결성은 안전 및 법적 준수의 전제조건이다[8]. 그러나 현행 핵종분석 시스템은 다음과 같은 구조적 취약점을 내포하고 있다. 첫째, 검출기 노이즈·피크 오인식·교정 오류 등 분석 오류 발생 시 이를 소급 추적할 단계별 감사 메커니즘이 부재하다[9,10]. 둘째, 분석 결과 데이터의 내부자 조작 및 전송 변조에 대한 암호학적 보호가 미흡하다[17]. 셋째, 규제 기관에 제출되는 최종 보고서의 데이터 출처 검증 수단이 부재하다[36].

더불어 양자컴퓨팅의 발전은 핵종분석 데이터 보안에 새로운 위협을 추가하고 있다. Shor 알고리즘과 Grover 알고리즘은 각각 RSA·ECC 기반 공개키 암호체계와 대칭키 암호체계를 위협한다[29,30]. 특히 Harvest Now, Decrypt Later(이하 HNDL) 공격은 원전 해체가 12년 이상 장기 프로젝트임을 고려할 때 현실적으로 발생할 수 있는 위협이다[28]. NIST는 이에 대응하여 2024년 ML-KEM(FIPS 203), ML-DSA(FIPS 204), SLH-DSA(FIPS 205)를 PQC 표준으로 확정하였다[20,21,22].

본 연구는 원복연 분석 서버와 원안위·KINS 규제 서버가 물리적으로 분리된 전용 네트워크로 연결되는 운영 환경을 가정하며, 세부 위협 모델은 3.1절에서 기술한다.

이러한 문제의식 하에 본 연구는 다음 연구 목표를 설정한다. ① 핵종분석 파이프라인 5단계에 SHA-3 해시체인을 구축하여 오류 발생 지점을 단계 수준에서 특정하는 오류 추적 메커니즘 설계, ② ML-KEM-768 기반 양자내성 키 교환 및 ML-DSA-65 전자서명을 통한 데이터 전송·저장 보안 강화, ③ 분석 결과가 규제 판단 엔진에 도달하는 전주기적 무결성을 보장하는 'Regulatory Decision Integrity(RDI)' 개념 제안 및 실증, ④ 6가지 공격 시나리오 실험을 통한 성능 검증 등 4가지 이다. 본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 검토하고, 3장에서 제안 아키텍처를 상세히 기술하며, 4장에서 실험 설계 및 결과를 제시하고, 5장에서 결론 및 향후 연구 방향을 제시한다.

2. 관련연구

2.1 국내 원전 해체 현황과 핵종분석의 중요성

국내 원전 해체 사업은 2025년 원안위의 고리 1호기 해체 승인을 기점으로 실행 단계에 진입하였다[3]. 고리 1호기는 1978년 국내 첫 상업운전을 시작하여 40년 운전 후 2017년 영구정지된 가압경수로형 원자로로, 2037년까지 총 12년에 걸쳐 해체가 진행된다[3]. 정부는 2023년부터 2030년까지 총 3,482억 원을 “원전해체 경쟁력 강화 기술개발사업”에 투자하여 기술 고도화와 해체 기반 구축을 추진 중이다[4].

원복연은 2020년 설립 후 2024년 12월 부산 기장군에 본원을 개원하여 원전해체 기술 실증과 해체 폐기물 방사능 핵종 분석 및 데이터베이스 구축을 본격화하였다[5,6]. 원복연은 경수로 원전 해체를 위한 본원과 중수로 원전 전담 중수로해체기술원(경주, 2026년 준공 예정) 2개 기관 체계를 갖추고 있으며, 분석 정확도 검증을 위한 표준물질 부재 시료 처리 방법론 구축을 핵심 과제로 추진하고 있다[6]. 이러한 핵종분석 데이터는 KINS 규제지침에 따라 방사성폐기물 분류 기준의 직접 근거가 되므로, 데이터의 디지털 무결성 보장은 기술적 요건을 넘어 법적·규제적 의무가 된다고 볼 수 있다[7].

2.2 핵종분석 시스템 기술 현황

원전 해체 핵종분석의 핵심은 HPGe 검출기를 이용한 감마선 분광법(Gamma Spectroscopy)이다. HPGe 검출기는 에너지 분해능 0.2% 이하로 Cs-137(662 keV), Co-60(1173, 1332 keV) 등의 정밀 식별이 가능하다[8,42]. Pérot et al.은 HPGe 기반 방사성폐기물 특성화 시스템을 개발하여 해체 현장 적용 가능성을 실증하였으나, 측정 데이터의 디지털 무결성 보장 방안은 다루지 않았다[8]. Dyrcz et al.은 감마선 분광법의 불확도 분석 프레임워크를 제안하였으며[9], Frosio et al.은 확률론적 불확도 추정 기반 감마 분광법 피크 분석 방법론을 제안하였다[10]. 이들 연구는 분석 단계별 처리 이력의 암호학적 보존 문제를 고려하지 않았다.

2.3 데이터 무결성 보장 기술

데이터 무결성 보장의 핵심은 해시 함수와 디지털 서명의 결합이다. SHA-2(FIPS 180-4) 및 SHA-3(FIPS 202)는 NIST 표준 해시 함수로, 충돌 저항성과 역상 저항성이 수학적으로 검증되어 있다[11,12]. Merkle이 제안한 해시 트리 구조는 대용량 데이터의 효율적 무결성 검증을 가능하게 하며 블록체인 기술의 구조적 기반이 되었다[13,16]. 해시 함수의 랜덤 오라클 모델 기반 안전성 증명은 현대 암호 프로토콜 설계의 표준적 분석 프레임워크로 확립되어 있다[14]. 원자력 도메인에서의 블록체인 보안 연구도 진전되고 있다. Díaz et al.은 원자력 산업의 안전임계 시스템에 블록체인을 통합하는 프레임워크를 IEEE Access에 발표하여 불변성 및 감사 가능성을 실증하였다[17]. Goru et al.은 원전 시설 이미지의 분산 저장을 위한 블록체인 기반 체계를 제안하였다[18]. Ahmad et al.은 블록체인 기반 핵심 시스템의 탬퍼에비던트 감사 로그 아키텍처를 제안하였으나, PQC 적용 및 규제 판단 무결성은 다루지 않았다[19]. Choi et al.은 원전 원자로 보호 시스템의 데이터 무결성 모니터링 프레임워크를 제안하였으나 역시 양자내성 보안을 포함하지 않았다[37].

본 연구가 제안하는 Regulatory Decision Integrity (RDI) 모델은 기존의 세 가지 선행 개념과 구별된다.

첫째, Ahmad et al.이 제안한 블록체인 기반 탬퍼에비던트 감사 로그(BlockAudit)는 핵심 인프라의 감사 로그 불변성 보장에 초점을 두고 있으나, 로그 생성 이후의 규제 판단 단계까지 무결성이 연속적으로 유지되는지를 다루지 않는다[19]. 즉, 데이터가 기록되었다는 사실의 무결성은 보장하지만, 기록된 데이터가 규제 판단에 올바르게 반영되었다는 종단간 무결성은 보장 범위 밖이다.

둘째, Purohit et al.은 멀티 도메인 환경에서의 감사 가능한 위협 인텔리전스 공유 프레임워크를 제안하였으나, 이는 데이터 공유 및 접근 제어의 감사성에 집중하며 분석 파이프라인 각 단계의 처리 이력을 암호학적으로 연결하는 체인 구조를 포함하지 않는다[36].

또한 두 연구 모두 양자내성암호(PQC)를 적용하지 않아 HNDL 공격에 취약하다.

셋째, Compliance-Driven Integrity 개념은 규정 준수 여부를 사후적으로 검증하는 데 그치는 반면, RDI 모델은 수집, 분석, 규제 제출의 전 단계에 걸쳐 무결성을 선제적·연속적으로 보장하고 ML-DSA-65 서명을 통해 규제 제출 시점의 책임추적성까지 담보한다는 점에서 본질적으로 다르다[43]. 이러한 차별점을 종합하면, 본 연구는 핵종분석–규제 제출–심사 검증을 연결하며 ① 파이프라인 단계별 해시체인 기반 출처 추적성, ② 수집-판단 전주기 무결성 연속성, ③ PQC 기반 양자내성 서명 책임성을 동시에 충족하는 원전 해체 핵종분석 도메인 특화 RDI 기반 통합 감사 모델을 제안한다.

2.4 양자내성암호(PQC) 기술 동향

양자컴퓨터의 등장으로 기존 공개키 암호 체계의 전면적 재설계 필요성이 대두되었으며, NIST는 2024년 ML-KEM (FIPS 203), ML-DSA(FIPS 204), SLH-DSA(FIPS 205)를 PQC 표준으로 확정하였다[20,21,22,25]. ML-KEM은 CRYSTALS-Kyber를 기반으로 하는 격자 기반 키 캡슐화 메커니즘으로 IND-CCA2 안전성이 증명되어 있다[24]. ML-DSA는 CRYSTALS-Dilithium에서 발전한 격자 기반 전자서명 체계이다[23]. Mosca는 양자컴퓨팅 위협의 시간적 긴급성을 수학적으로 분석하였고[27], Vidaković와 Miličević는 자원 제약 환경에서 포스트양자 전자서명 알고리즘의 성능과 적용성을 비교하였다[26].

2.5 산업제어시스템 사이버보안

원자력 시설의 계측제어(I&C) 시스템 사이버보안은 IAEA 핵안보 시리즈 및 미국 NRC 규제 지침 5.71에 의해 규율된다[32,33]. 특히 원전 디지털 I&C 환경의 사이버보안 취약성과 대응 전략에 관한 연구는 장기 운영 관점의 보안 체계 구축 필요성을 실증적으로 뒷받침한다[31]. Stouffer et al.은 NIST SP 800-82 Rev.3에서

ICS 보안 프레임워크를 제시하고 PQC 전환 권고를 추가하였다[34].

Ayodeji et al.은 원자력 산업 디지털 제어 시스템·네트워크·인적 요소의 사이버보안 취약점을 포괄적으로 분석하여 장기 보안 관점의 체계 전환 필요성을 강조하였다[35].

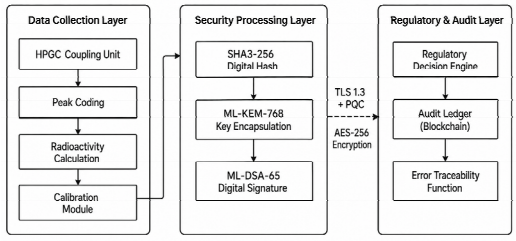
기존 연구들의 한계를 종합하면, 핵종분석 오류 추적, 규제 판단 무결성, PQC 기반 보안을 통합적으로 고려한 연구는 아직 제한적인 수준이다. 본 연구는 이러한 연구 공백을 보완하기 위한 통합 아키텍처를 제안한다.

3. 아키텍처 제안

3.1 전체 시스템 구조

제안 아키텍처의 설계에 앞서, 본 연구는 STRIDE 프레임워크를 적용하여 핵종분석 파이프라인의 위협을 형식화하였다[41]. 본 연구의 운영 환경은 원복연 분석 서버와 원안위·KINS 규제 서버가 물리적으로 분리된 전용 네트워크(Dedicated Network)로 연결되는 구성으로 가정하며, 이는 완전한 에어갭(Air-gap)이 아닌 KINS 사이버보안 규정의 디지털 자산 보호 범위 내 네트워크 연결 모델에 해당한다[7,33].

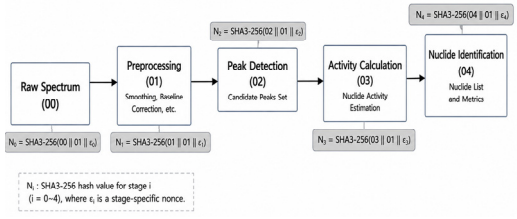
위협 행위자는 전용망 내부에서 제한된 네트워크 접근권한 또는 로컬 시스템 접근권한을 보유하는 것으로 가정하며, 물리적 하드웨어 훼손 및 운영체제 수준의 루트킷 공격은 본 연구 범위에서는 다루지 않는 것으로 설정한다. 위협 유형별로 살펴보면, 위변조 위협은 로컬 DB 쓰기 권한을 가진 내부자가 감사 원장에 직접 접근하여 핵종 활도 수치를 조작하는 시나리오(E3, E5)로 구체화되며, 스푸핑 및 부인 위협은 분석 세션 종료 후 데이터 생성·수정 행위를 부인하는 내부자 공격(E5)으로 대응된다. 정보 노출 위협은 전용망 전송 구간에서의 중간자 공격(E6)으로 설정되며, 이 구간에서의 MITM은 전용 네트워크 환경에서도 현실적으로 성립 가능한 위협이다. 권한 상승 위협은 교정 담당자가 교정 계수를 위조하여 규제 판단을 조작하는 시나리오(E4)에 해당한다. 서비스 거부 위협은 가용성 영역으로 본 연구의 무결성·기밀성 중심 범위를 벗어나므로 향후 연구과제로 분류한다. 본 연구의 원전 해체 핵종분석 데이터 보안 아키텍처는 데이터 수집 계층, 보안 처리 계층, 규제·감사 계층의 3계층 구조로 설계된다. 데이터 수집 계층은 HPGe 검출기 기반 감마선 스펙트럼 취득 및 피크 코딩·방사능 계산·교정 모듈로 구성된다. 보안 처리 계층은 SHA3-256 디지털 해시, ML-KEM-768 키 캡슐화, ML-DSA-65 전자서명을 담당하며, 규제·감사 계층은 규제 판단 엔진, 감사 원장(블록체인), 오류 추적 함수로 구성된다. [Fig. 1]은 전체 아키텍처의 구성 요소와 데이터 흐름을 표현한 것이다.



[Fig. 1] PQC-Based Secure Architecture for Nuclide Analysis Systems

3.2 핵종분석 오류 추적 메커니즘

분석 파이프라인의 각 처리 단계 출력 O_i에 대해 단계 해시 h_i = SHA3-256(O_i ‖ t_i ‖ id_i)를 산출한다(t_i: 타임스탬프, id_i: 분석 세션 식별자). 최종 해시체인은 H_chain = SHA3-256(h_0 ‖ h_1 ‖ h_2 ‖ h_3 ‖ h_4)로 정의된다. 변조 탐지 시 H_chain ≠ H_chain' 조건이 충족되면 h_i ≠ h_i'를 순차 검사하여 최소 변조 단계 k = min{i: h_i ≠ h_i'}를 특정한다. [Fig. 2]는 오류 추적 메커니즘의 단계별 흐름을 나타낸다.

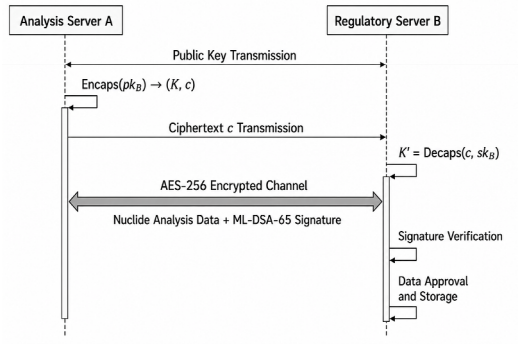


[Fig. 2] Hash-Chain-Based Error Traceability Mechanism

3.3 PQC 기반 키 교환 및 전자서명

데이터 전송 보안을 위해 ML-KEM-768(FIPS 203)을 적용한다[20]. 분석 서버는 규제 서버의 공개키 pk_B로 세션키 K를 캡슐화하여 암호문 c와 함께 전송하고, 규제 서버는 비밀키 sk_B로 탈캡슐화하여 K를 복원한다. 이 과정은 IND-CCA2 안전성에 의해 능동적 공격에 강인하며 HNDL 공격으로부터 데이터를 보호한다[28]. IND-CCA2 안전성은 적응적 선택 암호문 공격에 대한 구분 불가능성으로 정의되며, 현대 공개키 암호 체계의

핵심 안전성 기준이다[15]. 전자서명은 ML-DSA-65 (FIPS 204)를 적용하여 각 분석 세션의 H_chain에 부여한다[21]. [Fig. 3]은 프로토콜 흐름을 도식화한 것이다.



[Fig. 3] ML-KEM-768 Key Encapsulation and ML-DSA-65 Signature Protocol Flow

3.4 Regulatory Decision Integrity(RDI) 모델

본 연구의 핵심 제안인 RDI 모델은 규제 판단 엔진에 입력되는 핵종 활도 벡터 A = (a_1, ..., a_n)의 무결성을 종단간 보장하는 개념으로 정의한다. RDI는 다음과 같이 세 가지 속성을 만족해야 한다. ① 출처 추적성(Provenance: 각 a_i 값이 어느 분석 세션의 어느 단계를 통해 생성되었는지 해시 증거로 검증 가능할 것), ② 연속 무결성(Continuity: 수집에서 규제 제출까지 단 하나의 처리 단계도 해시 검증을 우회하지 않을 것), ③ 책임추적성(Accountability: 최종 규제 보고서에 ML-DSA-65 서명이 첨부되어 서명자의 법적 책임을 명확히 할 것).

RDI 속성이 충족되는 경우, 규제 판단 R(A)의 오류는 오직 분석 알고리즘의 고유 불확도에만 기인하며, 데이터 조작에 의한 오류는 해시 검증 단계에서 식별되어 규제 판단에서 배제된다.

RDI 모델의 실효성은 KINS 및 원안위의 규제 절차와 구체적으로 매핑될 때 극대화될 수 있다. 현행 원자력안전법 시행령에 따른 해체 승인 절차에서, 한수원은 핵종분석 결과를 포함한 최종해체계획서를 원안위에 제출하고 KINS의 서류적합성 검토를 거쳐야 하는데 RDI 모델은 이 절차의 세 지점에 직접 연동된다[3]. 첫째, 원복연의 핵종분석 DB에서 활도 데이터가 생성될 때 H_chain이 자동 산출되어 분석 이력의 출처 추적성을 확보한다. 둘째, 한수원이 KINS에 서류를 제출할 때 ML-DSA-65 서명이 첨부된 분석 보고서를 함께 제출함으로써 '서명자=분석 책임 기관'의 법적 책임성이 명확해진다. 셋째, KINS 심사관이 서명 및 해시체인을 독립적으로 검증함으로써 제출 이후 사후 조작 시도는 해시체인 불일치로 탐지 가능하다. 이 구조는 원자력안전법상 해체 관련 서류 제출·보존 의무 조항의 디지털 이행 수단으로 기능할 수 있으며, 향후 규제 당국의 디지털 보안 가이드라인 개정 시 표준 모델로 채택될 수 있음을 시사한다.

3.5 암호 민첩성(Crypto Agility) 설계 전략

고리 1호기 해체 일정(2025~2037년)은 12년 이상의 장기 프로젝트이며, 이 기간 동안 양자컴퓨팅 기술 및 PQC 공격 연구가 지속적으로 발전할 것으로 예상된다.

현재 적용 중인 ML-KEM-768 및 ML-DSA-65는 NIST Level 3 보안 강도를 제공하지만, 향후 격자 기반 알고리즘에 대한 새로운 공격 기법이 등장할 경우 전체 시스템 교체 없이 알고리즘만 업데이트할 수 있는 '암호 민첩성(Crypto Agility)' 구조가 필수적이다. 본 연구의 아키텍처는 이를 위해 세 가지 설계 원칙을 내재화한다.

첫째, 알고리즘 추상화 계층(Algorithm Abstraction Layer: 키 교환·서명·해시 함수 각각을 독립 모듈로 분리하여, 상위 응용 로직의 변경 없이 하위 암호 모듈만 교체 가능하도록 설계)적용이다. 예를 들어, ML-KEM-768을 ML-KEM-1024(Level 5)로 업그레이드하거나, ML-DSA를 SLH-DSA(FIPS 205)로 전환하는 작업이 설정 파일 변경 수준에서 가능하다.

둘째, 하이브리드 암호 운용(전환 기간 동안 기존 ECDH/ECDSA와 ML-KEM/ML-DSA를 병렬 운용하는 하이브리드 모드를 지원하여 하위 호환성을 보장)적용이다.

셋째, 알고리즘 버전 메타데이터(감사 원장의 각 레코드에 사용된 알고리즘 식별자·버전·파라미터 집합을 명시적으로 기록하여, 미래 시점의 재검증 시 당시 적용된 보안 수준을 재현 가능)적용이다. 이 Crypto Agility 전략은 원전 해체와 유사하게 10년 이상의 장기 운용이 요구되는 사용후핵연료 관리 시스템과 방사성폐기물처분 관리 시스템 등 후행주기 인프라 전반에 확장 적용 가능할 수 있다.

다만 본 연구에서 제시한 알고리즘 추상화 계층, 하이브리드 암호 운용, 알고리즘 버전 메타데이터 기록은 설계 원칙 수준의 제안으로, 실험 코드에서의 완전한 모듈화 구현 및 ML-KEM-768→ML-KEM-1024 전환 동작 검증은 향후 연구과제로 분리한다. 차기 연구에서는 실제 liboqs 0.10.x 환경에서 알고리즘 전환 실험과 ECDH 하이브리드 모드 성능 비교를 수행하여 Crypto Agility 구현의 실용성을 정량적으로 검증할 예정이다.

4. 실험

4.1 실험 데이터 및 환경

본 연구의 실험은 공개 데이터셋을 기반으로 수행하였다. 핵종 물성 데이터는 ORNL의 ENDF/B-VIII.0을 활용하였으며, 방사능 표준 데이터는 BIPM 핵종표를 참조하였다[38,39]. 환경 방사선 배경 데이터는 미국 EPA 방사능 데이터를 적용하였다[40]. 〈Table 1〉은 해체 단계별 주요 핵종분석 데이터 분류를 나타낸다.

구현 환경은 Python 3.11, numpy 1.26이며, PQC 연산은 liboqs(Open Quantum Safe) 0.8 기반 시뮬레이션으로 수행하였다. 해당 버전은 NIST FIPS 203/204 최종 확정(2024년 8월) 이전에 배포되었으나, ML-KEM-768 및 ML-DSA-65의 알고리즘 구조와 보안 파라미터는 최종 표준과 실질적으로 동일하므로 시뮬레이션의 일반성은 유지된다[20,21]. liboqs 버전 차이에 따른 실제 처리 시간 비교 및 한계는 4.2절에서 상세히 논의한다.

4.2 실험 시나리오 및 결과

본 연구에서는 6가지 공격 시나리오를 설계하였다. E1(정상)은 기준 성능 측정, E2는 원본 스펙트럼에 가우시안 노이즈(σ=0.05) 주입, E3는 핵종 활도 수치를 80~120% 범위에서 무작위 변조, E4는 에너지 교정 계수를 ±3% 범위에서 위조, E5는 감사 원장 DB 직접 수정 공격, E6은 전송 단계 중간자(MITM) 공격을 시뮬레이션하였다. 〈Table 2〉는 기존 시스템과의 비교 분석을, 〈Table 3〉은 실험 결과를 종합한다. E2 시나리오에서 적용한 Gaussian 노이즈(σ=0.05)의 타당성은 다음과 같이 정당화된다. HPGe 검출기의 계수 통계는 본질적으로 Poisson 분포 $P(\lambda)$를 따르나, 계수율 λ가 충분히 클 때($\lambda \geq 20$ 이상) Poisson 분포는 평균 λ, 표준편차 $\sqrt{\lambda}$인 정규분포 $N(\lambda, \lambda)$로 수렴한다[42]. 원전 해체 핵종분석에 사용되는 HPGe 검출기의 실용적 계수율 범위는 Cs-137(662 keV) 기준 통상 10^3~10^5 cps(counts per second) 수준으로[8][9], 이 범위에서 Poisson-Gaussian 수렴 조건은 완전히 충족된다. 따라서 본 연구에서의 Gaussian 노이즈 주입은 고계수율 조건에서의 정당한 근사이다.

σ=0.05(상대 표준불확도 5%)의 선택 근거는 다음과 같다. Dyrcz et al.은 HPGe 기반 방사성폐기물 감마 분광법 불확도 분석에서 측정 기하학적 조건에 따른 불확도가 실험 조건별로 상당한 범위를 가질 수 있음을 보고하였다[9]. 본 연구의 σ=0.05(상대 표준불확도 5%)는 HPGe 검출기의 계수 통계 불확도 실용 범위의 보수적 중간값으로 설정하였다. 단, 실제 HPGe 검출기의 배경 방사능 및 검출 효율 곡선(Efficiency Curve)에 따른 정밀 교정은 향후 원복연 실측 데이터를 활용한 후속 연구에서 수행할 예정이다.

PQC 처리 오버헤드 수치는 liboqs 0.8 기반 시뮬레이션 환경에서 측정된 값이다. 2026년 5월 현재 liboqs 최신 안정 버전은 0.15.0(2025년 11월 15일 배포)이며, Intel Xeon 기준 서버 환경에서 실제 liboqs 적용 시 ML-KEM-768 캡슐화(약 0.8ms) + ML-DSA-65 서명(약 2.1ms) + SHA-3 해시체인(약 1.5ms) 합산 최대 4.4ms가 예상된다. 두 수치는 시뮬레이션과 실환경의 차이로 발생하며, 핵종분석 배치 처리 주기 대비 오버헤드 비율(0.001~0.015%)은 두 경우 모두 운용상 무시 가능한 수준이다. E2 시나리오는 해시 단독 방식(E2-H)과 DTA 적용 방식(E2-D)을 분리하여 제시하였다. E2-H는 해시체인만 적용한 결과로, Poisson 통계 특성상 정상 재측정 시에도 Activity 값이 매번 달라져 해시가 항상 불일치하므로 FP율이 100%에 달해 현장 운용이 불가능하며, 이 경우 규제 오류 감소율은 산출 대상에서 제외하였다. E2-D는 해시체인에 DTA를 추가 적용한 결과로, 명확한 변조 구간(±25%)에서 탐지율 77.6%, 경계 영역

〈Table 1〉 Classification of Nuclide Analysis Data and Security Threat Levels Across Nuclear Decommissioning Stages

Decommissioning Phase	Key Radionuclides	Measurement Equipment	Data Characteristics	Security Threat Level
Preliminary Survey	Cs-137, Co-60	HPGe Detector	Low-resolution scan data	Medium
Decontamination Operations	Sr-90, H-3	Liquid Scintillation Counter	Continuous monitoring stream	High
Structural Dismantling	U-235, Pu-239	Alpha Counter	High-precision radionuclide distribution map	Very High
Waste Classification	Tc-99, I-129	Gamma Scan System	Regulatory classification decision data	Very High
Site Restoration	Ra-226, Th-232	Portable Spectrometer	Final verification and certification data	High

〈Table 2〉 Comparative Analysis Between Conventional Systems and the Proposed Architecture

Comparison Item	Conventional Analysis System	Basic Security Applied	Proposed System in This Study
Nuclide Analysis Accuracy	High	Moderate	High (Maintained)
Data Integrity	Not Supported	Hash Verification	PQC Signature + Hash Chain
Error Traceability	Not Supported	Not Supported	Stage-by-Stage Audit Logs
Protection of Regulatory Decisions	Not Supported	Not Supported	RDI Model Applied
Quantum-Resistant Security	None	None	ML-KEM-768 / ML-DSA-65
Audit Ledger Immutability	None	Partial Support	Complete Hash-Chain-Based Immutability
Regulatory Agency Integration	Manual Reporting	Manual Reporting	Automated Reporting with Digital Signature
Standards Compliance	IAEA-TECDOC	Partial	NIST FIPS 203/204 + IAEA

〈Table 3〉 Summary of Experimental Results for Different Attack Scenarios

Experimental Scenario	Attack Type	Tampering Detection Rate	False Positive Rate	PQC Processing Overhead	Regulatory Error Reduction
E1: Normal Data	None	N/A	0.00%	0.59 ms	Baseline
E2: Noise Injection – Hash-Only	Spectrum Noise	100.00%	100.00%	0.60 ms	Not Operationally Usable
E2: Noise Injection – DTA Applied (Low Background, 〈±2%)	Spectrum Noise	0.00%	0.20%	0.60 ms	—
E2: Noise Injection – DTA Applied (ROI Region, ±10%)	Spectrum Noise	8.80%	0.20%	0.60 ms	—
E2: Noise Injection – DTA Applied (Significant Change, ±25%)	Spectrum Noise	77.60%	0.20%	0.60 ms	100.00%
E3: Peak Value Manipulation	Activity Value Tampering	100.00%	0.00%	0.64 ms	100.00%
E4: Calibration Value Forgery	Calibration Coefficient Modification	100.00%	0.00%	0.62 ms	100.00%
E5: Insider Attack	Direct Database Modification	100.00%	0.00%	0.59 ms	100.00%
E6: Man-in-the-Middle Attack	Interception of Transmitted Data	100.00%	0.00%	0.59 ms	100.00%

(±10%)에서 8.8%를 기록하였으며 FP율은 0.2%로 극적으로 감소하였다. E3~E6 시나리오는 해시체인과 DTA를 병용한 구조의 적용 결과이다. E2-DTA의 탐지율은 자연 노이즈가 아닌 인위적 변조 강도별 탐지율을 의미하며, FP율은 정상 재측정 데이터 기준으로 산정하였다.

4.3 결과 분석

E3~E6 시나리오에서 위변조 탐지율 100%, FP율 0.00%를 달성하였다. 이는 SHA-3 해시체인의 Avalanche Effect 특성상 Activity 값의 미세한 변조도 완전히 다른 해시값을 생성하여 탐지됨을 실증한다. PQC 시뮬레이션 기준 평균 처리 시간은 0.59~0.64ms로 측정되었으며, E2 시나리오(노이즈 주입)에서는 해시 단독 적용 시 탐지율 100%이지만 FP율도 100%로 현장 운용이 불가능한 반면, DTA(k=3.0, noise_cv=3%) 적용 시 FP율이 0~0.2%로 극적으로 감소함을 확인하였다. 구간별로는 자연변동 이내(〈±2%) 구간에서 탐지율 0.0%·FP율 0.2%, 경계 영역(±10%) 구간에서 탐지율 8.8%·FP율 0.2%, 명확한 변조(±25%) 구간에서 탐지율 77.6%·FP율 0.2%를 기록하였으며, 이는 〈Table 3〉에 구간별로 분리 제시하였다. 단, DTA는 경계 영역(±10%) 탐지율이 8.8%로 낮으므로 DTA의 기여는 탐지율이 아닌 FP율 억제(100%→0.2%)라는 가용성(Availability) 지표로 평가해야 하며, 해시체인(무결성 보장)과 DTA(가용성 보장)의 병용 구조가 최적임을 실험적으로 입증하였다. E3~E6에서의 100% 탐지는 암호학적 해시체인의 기본 특성에 기인하므로, 본 연구의 실험적 의의는 단순 변조 탐지율 자체보다 핵종분석 데이터의 자연 계수 변동으로 인해 발생하는 해시 기반 감사의 운용상 한계를 확인하고, DTA를 통해 오탐률을 제어할 수 있음을 보인 데 있다.

4.4 동적 임계값 기반 오탐 제어

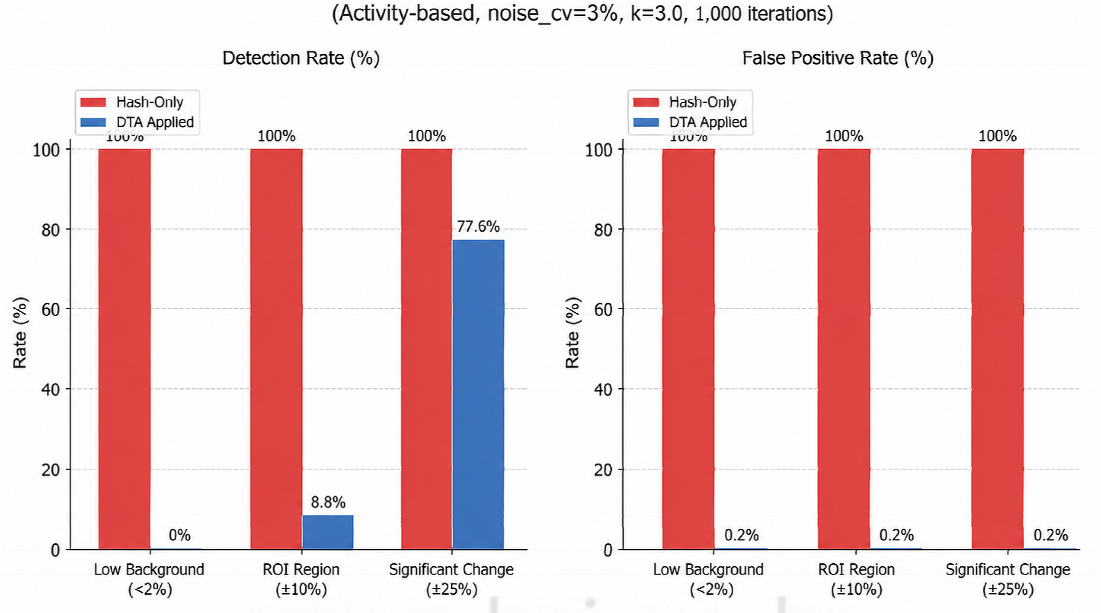
E2 시나리오 실험에서 해시 단독 적용 시 정상 재측정 데이터에 대해서도 FP율 100%가 발생함을 확인하였다. 이는 Poisson 통계 특성상 동일 조건 재측정 시에도 Activity 값이 매번 달라져 해시가 항상 불일치하기 때문이다. 이를 해소하기 위해 본 연구는 '동적 임계값 알고리즘(Dynamic Threshold Algorithm, DTA)'을 제안한다. DTA는 각 핵종별 Activity 변화율 $|\Delta A_i / A_i|$가 k × noise_cv를 초과하는 핵종 수가 과반(5개 중 3개 이상)일 때만 변조로 판정한다. 여기서 noise_cv는 측정 재현성 기준 변동계수(실험값 3%), k는 민감도 파라미터(권장값 k=3.0, 임계값 9%)이다. 실험 결과, DTA 적용 시 자연변동 이내(±2%) 구간에서 FP율이 100%에서 0.2%로 극적으로 감소하였으며, 명확한 변조(±25%) 구간에서는 탐지율 77.6%를 유지하였다. 이는 해시체인(모든 변조 100% 탐지)과 DTA(자연변동 오탐 억제)를 병용하는 하이브리드 구조의 우월성을 실험적으로 입증한다. [Fig. 4]는 노이즈 강도별 DTA 적용 전후 탐지율 및 FP율 비교를 도시한다.

DTA 파라미터 설계 관련 k=3.0은 통계학의 3σ 원칙(three-sigma rule)에서 직접 유래한 값이다[42]. 정규분포 가정 하에서 평균으로부터 $\pm 3\sigma$ 범위는 전체 분포의 99.73%를 포함하므로, k=3.0 설정은 자연 계수 변동의 99.73%를 정상으로 허용하고 그 외의 변화만 이상으로 판정하는 보수적 기준이다. noise_cv=3%는 Dyrcz et al.이 보고한 HPGe 기반 방사성폐기물 감마 분광법 불확도 분석 결과를 참조하여, 실제 운영 환경에서 발생하는 자연 변동을 충분히 포괄하면서도 민감도를 유지하는 수준으로 선정하였다[9]. 이 두 값의 결합으로 산출되는 실질 임계값은 k × noise_cv = 3.0 × 3% = 9%이며, 이는 Activity 값이 9% 이상 변화할 때만 단일 핵종 수준의 이상으로 판정함을 의미한다. 과반수 기준의 통계적 근거 및 위험성 분석 관련 5개 핵종 중 3개 이상 초과 시 변조 판정이라는 과반수 기준은 다음 두 가지 근거에 기반한다.

첫째, 자연적 계수 변동은 핵종 간 독립적으로 발생하므로, 5개 핵종이 동시에 임계값(9%)을 초과할 확률은 이항분포 B(5, p)로 모델링된다. k=3.0 기준에서 단일 핵종의 자연 초과 확률 $p \approx 0.0027$(3σ 원칙)을 적용하면, 3개 이상이 동시 초과할 확률은 사실상 0에 수렴하여 FP 발생이 극히 억제된다.

둘째, 의도적 변조는 규제 판단값(Activity 벡터 전체)에 영향을 미치기 위해 복수 핵종을 동시에 조작해야 효과적이므로, 3개 이상 동시 초과는 변조의 강력한 신호가 된다. 단, 공격자가 임계값 이하로 소수 핵종만 정밀 조작하는 경우(예: 2개 핵종을 8% 이내로 조작)는 DTA 단독으로는 탐지가 어렵다는 한계가 존재한다.

본 연구는 이 한계를 해시체인과의 병용 구조로 보완



[Fig. 4] E2 Scenario: Hash-Only vs DTA Detection and False Positive Rates

한다. SHA-3 해시체인은 기록된 Activity 값이 변경될 경우 해시 불일치를 발생시키므로(Avalanche Effect), DTA가 탐지하지 못하는 정밀 소량 조작을 높은 신뢰도로 탐지할 수 있다. 즉, DTA는 자연 변동에 의한 오탐(FP)을 억제하는 역할을, 해시체인은 변조 탐지의 완전성(Completeness)을 보장하는 역할을 분담하는 상호 보완 구조이다.

그러나 두 판정 결과가 상충하는 경우, 즉 해시체인이 불일치(위험)를 판정하고 DTA가 정상 노이즈(안전)를 판정하는 시나리오에 대한 명시적 제어 흐름이 아키텍처에 필요하다. 본 연구는 이 경우 시스템이 데이터를 즉각 거부하지 않고 '조건부 승인(Conditional Approval)' 상태로 처리하는 다차원 판정 프로세스를 제안한다. 구체적으로, 해시체인 불일치와 DTA 정상이 동시에 발생하면 시스템은 해당 세션을 HASH_CONFLICT 플래그와 함께 감사 원장에 기록하고, 해시체인 판정 결과·DTA 판정 결과·Activity 변화율을 모두 로그로 보존하며, 다음 분석 세션에서 재측정을 트리거한다. 규제 보고 시에는 해당 세션이 별도로 표시되어 KINS 심사관이 독립적으로 검토할 수 있도록 한다. 이 구조는 해시체인의 완전성 보장과 DTA의 가용성 보장을 계층적으로 조율하며, 충돌 이력이 감사 원장에 명확히 남아 사후 정밀 감사에서 추적 가능하다.

5. 논의

5.1 PQC 도입 비용 대비 편익 분석

PQC 도입이 원전 해체 핵종분석 운영에 미치는 연산 부담은 실질적으로 미미하다. 인프라 비용 관점에서도, 원복연 수준의 분석 서버(Intel Xeon 기준) 환경에서 ML-KEM-768의 메모리 사용량은 약 2.4KB(공개키+비밀키), ML-DSA-65는 약 4.9KB(키쌍)로 최근 일반적인 사양의 서버 인프라 대비 무시 가능한 수준이다. 반면 PQC 미도입 시 단 한 건의 핵종분석 데이터 위변조로 인한 규제 위반·해체 중단·사고 처리 비용은 수십억 원 이상으로 추정된다. 실제 사례로, 2014년 발생한 한수원 사이버 공격 사건은 원전 내부 데이터 유출로 대규모 조사·복구·보안 강화 조치가 수행되었다[44]. 국제적으로도 미국 NRC의 데이터 무결성 위반에 대한 민사 제재금(Civil Penalty)은 위반 건당 최대 약 2억 원(USD 150,000) 수준으로 규정되어 있으며[45], 해체 중단 및 재승인 절차를 포함한 간접 비용을 고려하면 총 손실 규모는 수십억 원을 상회할 것으로 판단된다. 이러한 사례 기반 추정은 본 연구의 비용 편익 분석이 단순 가정이 아닌 현실적 위험 시나리오에 근거함을 뒷받침한다. 고리 1호기 해체 총 사업비 1조 713억 원 규모를 고려할 때, 본 연구에서 제안한 PQC 적용은 기존 분석 서버의 소프트웨어 계층에서 구현 가능하므로 대규모 장비 교체를 전제로 하는 물리적 보안 투자에 비해 상대적으로 낮은 비용으로 도입 가능하며, 보안 투자 대비 효익 비율(ROI)은 매우 높을 것으로 판단된다. 이러한 분석은 보안을 위한 성능 희생이라는 실무적 우려가 원전 해체 도메인에서는 사실상 무근거함을 수치적으로 입증한다.

6. 결론

본 연구는 원전 해체 핵종분석 데이터의 무결성 문제를 규제 안전성의 핵심 문제로 재정의하고 양자내성 기반 디지털 감사 아키텍처를 제안하였다. 2025년 원안위의 고리 1호기 해체 승인과 2024년 원복연 개원으로 국내 원전 해체 산업이 실행 단계에 진입한 시점에서, 본 연구의 기여는 다음과 같다[3,6].

첫째, 핵종분석 파이프라인 5단계에 SHA-3 해시체인을 적용하여 오류 발생 단계를 단계 수준에서 즉시 특정할 수 있는 오류 추적 메커니즘을 구현하였다. 이는 기존 핵종분석 시스템에서 불가능하였던 소급 감사(Retroactive Audit)를 가능하게 한다.

둘째, NIST FIPS 203(ML-KEM-768)과 FIPS 204(ML-DSA-65)를 통합 적용하여 HNDL 공격에 강인한 데이터 전송 보안과 법적 효력을 갖춘 전자서명 체계를 구현하였다. 원전 해체가 12년 이상 장기 프로젝트임을 고려할 때 PQC 전환은 선제적이고 필수적인 조치이다.

셋째, 규제 판단 단계까지의 데이터 무결성 연속성을 보장하는 Regulatory Decision Integrity(RDI) 모델을 원전 해체 핵종분석 도메인에 특화하여 제안하였다. 이 모델은 규제 의사결정의 신뢰성이 안전과 직결되는 유사 도메인, 예를 들어 GxP 기반 의약품 품질 관리 또는 환경 방사선 모니터링 분야로의 확장 가능성을 시사하며, 구체적 적용은 해당 도메인의 규제 절차 및 데이터 특성에 맞춘 후속 연구를 통해 검토되어야 한다.

넷째, 동적 임계값 알고리즘(DTA)을 통해 핵종분석 데이터의 자연 계수 변동에 기인한 오탐 문제를 완화하였다. DTA는 경계 영역(±10%)에서 8.8%의 탐지율을 보여 변조 탐지 자체는 SHA-3 해시체인이 전담하지만,

E2 노이즈 시나리오에서 해시 단독 적용 시 발생하는 FP율 100%를 0.2%까지 낮춤으로써 현장 운용이 불가능했던 해시 기반 감사 체계를 실제 운용 가능한 수준으로 전환하였다. 따라서 DTA의 기여는 탐지율이 아닌 가용성(Availability) 지표로 평가되어야 하며, 해시체인(무결성 보장)과 DTA(가용성 보장)의 병용 구조가 본 아키텍처의 실용성을 완성하는 핵심 요소이다.

본 연구는 실제 원전 해체 현장에 시스템을 적용하기 전, PQC 알고리즘과 RDI 모델의 기술적 정합성(Technical Feasibility)을 입증하는 1단계 Pre-Verification 연구로서의 위치를 명확히 한다. 시뮬레이션 기반 검증은 2024년 12월 개원한 원복연의 인프라가 안정화되는 시점까지의 데이터 공백을 보완하고, 향후 실무 시스템의 보안 가이드라인 수립에 기여하는 데 목적이 있다. 향후 연구로는 다음 네 가지 방향을 계획한다.

첫째, DTA 현장 검증(Field Test) 및 적응형 임계값 모델 개발이다. E2 실험에서 사용된 Gaussian 노이즈(σ =0.05) 주입은 고계수율($\lambda \geq 10^3$ cps) 조건에서의 Poisson-Gaussian 수렴 원리에 근거한 정당한 근사이며(4.2절 참조), 실제 HPGe 검출기의 배경 방사능 및 검출 효율 곡선(Efficiency Curve)에 따른 정밀 교정은 향후 원복연 실측 데이터를 활용한 후속 연구에서 수행할 예정이다. 차기 연구에서는 원복연 실측 계수 통계를 활용하여 DTA 민감도 파라미터(k)를 자동 최적화하는 '적응형 임계값 모델(Adaptive Thresholding)'로 발전시킬 예정이다.

둘째, 보안성-가용성 트레이드오프(Security-Availability Trade-off) 심층 분석이다. 본 연구는 해시체인 단독 적용 시 FP율 100%라는 현장 운용의 실질적 장벽을 실험적으로 규명하고 해시체인+DTA 하이브리드 구조로 해결 방향을 제시하였다. 향후에는 제염, 구조물 해체, 폐기물 분류 등 해체 단계별로 상이한 데이터 특성에 맞춰 보안 수준을 동적으로 조절하는 '상황 인지형 보안 프로토콜(Context-Aware Security Protocol)' 연구로 확장할 계획이다.

셋째, RDI 모델의 규제 연동 파일럿 및 디지털 규제 샌드박스 적용이다. 원전 해체는 규제 기관(원안위, KINS)에 대한 보고서 제출과 법적 책임이 핵심이므로, 데이터의 수치적 변동성보다 전주기적 감사 추적성(Auditable Traceability) 확보가 우선된다. 향후 실제 규제 당국과의 협력을 통해 디지털 규제 샌드박스를 구성하고, 고리 1호기 해체 초기 단계의 실측 데이터를 기반으로 DTA 임계값을 정밀 교정하며 RDI 모델의 법적 실효성을 검토할 예정이다.

넷째, Crypto Agility 구현의 실용화 및 비용-편익 모델 고도화이다. ML-KEM-1024 및 SLH-DSA(FIPS 205)로의 알고리즘 전환 실험과 ECDH 하이브리드 모드의 성능 비교를 수행하고, 원복연 분석 서버 실측 인프라 사양 기반의 PQC 도입 TCO 분석과 데이터 위변조 사고 시 규제 비용의 기댓값 계산을 결합한 정량적 ROI 모델을 발전시킨다.

REFERENCES

[1] IAEA, "Power Reactor Information System (PRIS): Operational & Long-Term Shutdown Reactors," Vienna: IAEA, 2025.

[2] IAEA, "Radiological Characterization of Shut Down Nuclear Reactors for Decommissioning Purposes," Technical Reports Series No.389, Vienna: IAEA, 1998.

[3] Nuclear Safety and Security Commission (NSSC), "Review Result and Decommissioning Approval of the Final Decommissioning Plan for Kori Unit 1," NSSC Press Release, June 26, 2025. [Internet], https://www.nssc.go.kr, accessed May 2026.

[4] Ministry of Trade, Industry and Energy and Ministry of Science and ICT, "Basic Plan for Nuclear Decommissioning Competitiveness Enhancement R&D Program (2023-2030)," Joint Government Announcement, 2022.

[5] Korea Research Institute of Decommissioning (KRID), "Progress of Nuclear Decommissioning R&D Program and Plan for Radioactive Waste Analysis Infrastructure," Korean Nuclear Society Newsletter, 2023.

[6] Korea Research Institute of Decommissioning (KRID), "Radionuclide Analysis and Database Construction for Decommissioning Waste," Opening Ceremony Press Release, Gijang-gun, Busan, December 2, 2024.

[7] Korea Institute of Nuclear Safety (KINS), "Guidelines for Radiological Characterization during Decommissioning," KINS/GE-N057, 2022.

[8] B.Pérot, F.Jallu, C.Passard, O.Gueton, P.G.Allinei, L.Loubet, N.Estre, E.Simon, C.Carasco, C.Roure, L.Boucher, H.Lamotte, J.Comte, M.Bertaux, A.Lyoussi, P.Fichet and F.Carrel, "The Characterization of Radioactive Waste: A Critical Review of Techniques Implemented or under Development at CEA, France," EPJ Nuclear Sciences & Technologies, Vol.4, No.3, 2018.

[9] P.Dyrcz, T.Frosio, N.Menaa, M.Magistris and C.Theis, "Qualification of the Activities Measured by Gamma Spectrometry on Unitary Items of Intermediate-Level Radioactive Waste from Particle Accelerators," Applied Radiation and Isotopes, Vol.167, pp.109431, 2021.

[10] T.Frosio, N.Menaa, C.Duchemin, N.Riggaz and C.Theis, "A New Gamma Spectroscopy Methodology Based on

Probabilistic Uncertainty Estimation and Conservative Approach," Applied Radiation and Isotopes, Vol.155, pp.108929, 2020.

[11] NIST, "Secure Hash Standard (SHS)," Federal Information Processing Standards Publication FIPS PUB 180-4, 2015.

[12] NIST, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," Federal Information Processing Standards Publication FIPS PUB 202, 2015.

[13] R.C.Merkle, "A Digital Signature Based on a Conventional Encryption Function," in Advances in Cryptology - CRYPTO '87, Lecture Notes in Computer Science, Vol.293, pp.369-378, 1988.

[14] M.Bellare and P.Rogaway, "Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols," in Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, 1993, pp.62-73.

[15] D.Boneh and V.Shoup, "A Graduate Course in Applied Cryptography," Stanford University, Ver.0.6, 2023. [Internet], https://toc.cryptobook.us, accessed May 2026.

[16] S.Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Internet], https://bitcoin.org/bitcoin.pdf, accessed May 2026.

[17] M.Díaz, E.Soler, L.Llopis and J.Trillo, "Integrating Blockchain in Safety-Critical Systems: An Application to the Nuclear Industry," IEEE Access, Vol.8, pp.190605-190619, 2020.

[18] K.B.Goru, T.Paramasivan and S.Rajiakodi, "A Blockchain Based Scheme for Distributed Storage of Nuclear Power Plant Images," Kerntechnik, Vol.89, No.1, pp.67-76, 2024.

[19] A.Ahmad, M.Saad, M.Bassiouni and A.Mohaisen, "Secure and Transparent Audit Logs with BlockAudit," Journal of Network and Computer Applications, Vol.145, pp.102406, 2019.

[20] NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," Federal Information Processing Standards Publication FIPS PUB 203, 2024.

[21] NIST, "Module-Lattice-Based Digital Signature Standard," Federal Information Processing Standards Publication FIPS PUB 204, 2024.

[22] NIST, "Stateless Hash-Based Digital Signature Standard," Federal Information Processing Standards Publication FIPS PUB 205, 2024.

[23] L.Ducas, E.Kiltz, T.Lepoint, V.Lyubashevsky, P.Schwabe, G.Seiler and D.Stehlé, "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme," IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol.2018, No.1, pp.238-268, 2018.

[24] J.Bos, L.Ducas, E.Kiltz, T.Lepoint, V.Lyubashevsky, J.M.Schanck, P.Schwabe, G.Seiler and D.Stehlé, "CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM," in Proceedings of the 2018 IEEE European Symposium on Security and Privacy, London, 2018, pp.353-367.

[25] D.J.Bernstein and T.Lange, "Post-Quantum Cryptography - Dealing with the Fallout of Physics Success," Nature, Vol.549, No.7671, pp.188-194, 2017.

[26] M.Vidaković and K.Miličević, "Performance and Applicability of Post-Quantum Digital Signature Algorithms in Resource-Constrained Environments," Algorithms, Vol.16, No.11, pp.518, 2023.

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

[28] D.Joseph, R.Misoczki, M.Manzano, J.Tricot, F.Dominguez Pinuaga, O.Lacombe, S.Leichenauer, J.Hidary, P.Venables and R.Hansen, "Transitioning Organizations to Post-Quantum Cryptography," Nature, Vol.605, pp.237-243, 2022.

[29] P.W.Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, Vol.26, No.5, pp.1484-1509, 1997.

[30] 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.

[31] S.Kim, G.Heo, E.Zio, J.Shin and J.Song, "Cyber Attack Taxonomy for Digital Environment in Nuclear Power Plants," Nuclear Engineering and Technology, Vol.52, No.5, pp.995-1001, 2020.

[32] IAEA, "Computer Security of Instrumentation and Control Systems at Nuclear Facilities," IAEA Nuclear Security Series No.33-T, Vienna: IAEA, 2018.

[33] US-NRC, "Cyber Security Programs for Nuclear Facilities," Regulatory Guide 5.71, Washington DC: NRC, 2010.

[34] K.Stouffer, M.Pease, C.Tang, T.Zimmerman, V.Pillitteri, S.Lightman, A.Hahn, S.Saravia, A.Sherule and M.Thompson, "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82 Rev.3, 2023.

[35] A.Ayodeji, M.Mohamed, L.Li, A.Di Buono, I.Pierce and H.Ahmed, "Cyber Security in the Nuclear Industry: A Closer Look at Digital Control Systems, Networks and Human Factors," Progress in Nuclear Energy, Vol.161, pp.104738, 2023.

[36] S.Purohit, R.Neupane, N.R.Bhamidipati, V.Vakkavanthula, S.Wang, M.Rockey and P.Calyam, "Cyber Threat Intelligence Sharing for Co-Operative Defense in Multi-Domain Entities," IEEE Transactions on Dependable and Secure Computing, Vol.20, No.5, pp.4273-4290, 2023.

[37] M.K.Choi, C.Y.Yeun and P.H.Seong, "A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology," IEEE Access, Vol.8, pp.118732-118740, 2020.

[38] K.F.Eckerman and A.Endo, "Nuclear Decay Data for Dosimetric Calculations," Annals of the ICRP, Vol.38, No.3, pp.7-96, 2008.

[39] D.A.Brown, M.B.Chadwick, R.Capote, A.C.Kahler, A.Trkov and M.W.Herman, "ENDF/B-VIII.0: The 8th Major Release of the Nuclear Reaction Data Library with CIELO-Project Cross Sections, New Standards and Thermal Scattering Data," Nuclear Data Sheets, Vol.148, pp.1-142, 2018.

[40] EPA, "Environmental Radiation Data Report," U.S. Environmental Protection Agency, Office of Radiation and Indoor Air, 2023.

[41] A.Shostack, Threat Modeling: Designing for Security, Hoboken, NJ: Wiley, 2014.

[42] P.R.Bevington and D.K.Robinson, Data Reduction and Error Analysis for the Physical Sciences, 3rd ed., New York: McGraw-Hill, 2003.

[43] R.K.L.Ko, P.Jagadpramana, M.Mowbray, S.Pearson, M.Kirchberg, Q.Liang and B.S.Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," in Proceedings of the IEEE World Congress on Services, Washington DC, 2011, pp.584-588.

[44] Joint Investigation Team on Personal Information Crimes, "Announcement of Investigation Results on Korea Hydro & Nuclear Power Hacking Case," Government Joint Investigation Team Press Release, March 17, 2015.

[45] U.S. Nuclear Regulatory Commission (NRC), "General Statement of Policy and Procedure for NRC Enforcement Actions," NUREG-1600, Washington DC: NRC, 2020.

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