정 보 보 호 학 회 지
제34권 제6호, 2024. 12

국내·외 양자내성암호 표준화 및 전환 정책 동향 분석

양 유 진*, 송 강 수**, 손 기 종***

요 약

양자컴퓨터의 발전으로 기존 암호체계에 대한 보안 위협 가능성이 높아지면서, 양자내성암호의 중요성이 더욱 강조되고 있다. 양자내성암호는 양자컴퓨터의 위협에도 안전성을 유지할 수 있는 기술로, 현재 주요 국가들은 표준화와 단계적 전환을 추진하며 국가의 정보보호 역량 강화를 도모하고 있다.

본 논문은 한국의 효과적인 양자내성암호 전환 방안을 모색하기 위해 미국, 유럽, 일본, 중국 등 주요 국가의 양자내성암호 전환 동향과 한국의 전환 현황을 분석한다.

Ⅰ. 서 론

양자역학의 얽힘(entanglement)과 중첩(super-position) 현상을 활용하여 설계된 양자컴퓨터는 특정 계산 문제에서 기존의 고전 컴퓨터를 압도할 수 있는 능력을 가지고 있어 암호학 분야에 중대한 변화를 불러올 것으로 예측되고 있다. 특히, 쇼어 알고리즘(Shor's Algorithm)[1]과 같은 양자 알고리즘은 소인수분해, 이산대수 문제 등을 기반으로 하는 기존 공개키 암호 체계(RSA, ECC 등)를 무력화할 가능성을 제시하며 새로운 암호 체계의 필요성을 대두시켰다. 이러한 배경에서 등장한 기술이 바로 양자내성암호(Post-Quantum Cryptography, PQC)이다. 양자내성암호는 양자컴퓨터의 위협에도 안전성을 유지할 수 있는 암호 기술로, 양자컴퓨터 연구의 진전과 암호학적으로 유의미한 양자컴퓨터의 개발 가능성이 높아짐에 따라[2] 국제 사회에서 그 중요성과 필요성이 점차 강조되고 있다.

현재 주요 국가들은 양자내성암호의 표준화를 가속화하고 단계적인 전환을 추진하고 있다. 특히, 미국, 유럽 등은 정부 주도로 표준화 작업을 이끌며 정책적, 기술적 지원을 통해 안정적인 암호 전환을 도모하고 있다. 이러한 움직임은 단순히 기술적인 대안을 마련하는 것을 넘어, 국가의 정보보호 역량을 강화하고 디지털 경제의 지속 가능성을 확보하기 위한 전략적 과제로 인식되고 있다.

본 논문은 한국이 양자내성암호 전환의 구체적인 이정표를 마련하는 데 기여하기 위해 양자내성암호 전환을 선도하고 있는 주요 국가들의 최신 표준화 및 전환 정책 동향을 분석하고, 한국의 전환 현황을 살펴본다.

Ⅱ. 국외 양자내성암호 표준화·전환 정책 동향

본 장에서는 미국, 유럽, 일본 등 국가 차원에서 양자내성암호로의 전환을 추진 중인 주요 국가들의 양자내성암호 표준화 현황과 전환 정책의 동향을 종합적으로 분석한다.

2.1. 미국

미국은 양자내성암호 전환을 주도하는 핵심 국가 중 하나이다. [3]에 소개된 내용을 바탕으로 전환 정책의 최신 동향을 순차적으로 살펴본다. 논의에 앞서 자주 등장하는 용어를 [표 1]에 정리하였다.

〔표 1〕 자주 등장하는 용어/약어 설명

용어	설명
CRQC	Cryptanalytically-Relevant Quantum Computer : 기존 공개키 암호 알고리즘(RSA, ECC 등)을 약화시킬 수 있는 양자컴퓨터

* 한국인터넷진흥원 차세대암호기술팀 (주임연구원, yangyu34@kisa.or.kr)
** 한국인터넷진흥원 차세대암호기술팀 (수석연구원, ksong@kisa.or.kr)
*** 한국인터넷진흥원 차세대암호기술팀 (팀장, skj@kisa.or.kr)

용어	설명
ACDI	Automated Cryptography Discovery & Inventory : 시스템, 네트워크에서 사용되는 암호 알고리즘·자산 탐지 및 관련 정보 수집을 자동으로 수행하는 기술
CDM	Continuous Diagnostics and Mitigation : 美 연방 정부가 사용하는 시스템, 네트워크의 보안 상태를 관리하는 프로그램
CNSA	Commercial National Security Algorithm Suite : 국가안보국(NSA)이 국가안보시스템(NSS)의 보안 강화를 위해 개발한 암호화 알고리즘 집합 표준

2.1.1. 표준화

미국은 국립표준기술연구원(National Institute of Standards and Technology, NIST)을 주축으로 양자내성암호 알고리즘 표준화 작업을 진행하고 있다.

표준화 작업에 앞서 NIST는 2016년 12월, 양자내성암호 표준화 공모전을 개최했으며, 2022년 7월 4개의 알고리즘(1개 PKE/KEM, 3개의 전자서명)을 표준화 대상 알고리즘으로 선정하였다[4]. NIST는 격자 기반(Lattice-based) 알고리즘에만 의존하지 않고 알고리즘의 다양성을 확보하기 위해 4개의 非 격자 기반 대체 알고리즘을 선정하여 추가 라운드(4라운드)를 진행하고 있다[4]. 그러나 이 중 아이소제니 기반(Isogeny-based) 알고리즘인 SIKE는 2023년 8월 보안 취약점이 발견되어 제외되었다[5]. 현재는 3개의 코드 기반(Code-based) 알고리즘(BIKE, Classic McEliece, HQC)에 대한 검토가 진행 중이며[4] 2024년 말까지 1~2개가 대체 알고리즘이 최종 선정될 예정이다[6].

또한, 2022년 7월에는 전자서명 알고리즘의 다양성을 확보하기 위해 추가적인 전자서명 알고리즘 공모가 개최되었으며, 2023년 6월에 공개된 40개의 1라운드 진출 후보 알고리즘 중 14개가 2024년 10월에 2라운드로 진출하였다. 계획에 따르면, 3라운드 후보는 2026년에 선정될 예정이다[7].

최종 선정된 표준화 대상 알고리즘 중 3개는 2023년 8월 표준 초안이 공개된 이후 2024년 8월 미국 연방정보처리표준(Federal Information Processing Standards, FIPS)으로 최종 채택되었다. FN-DSA (FALCON)는 2024년 8월 표준화 작업을 시작하여 2024년 말 표준 초안 공개를 목표로 표준화 작업을 진행 중이다. 각 알고리즘은 표준화 작업 과정에서 이름에 버전을 명시하도록 변경되었으며, 각 알고리즘에 따른 관련 표준 문서번호는 [표 2]에 정리하였다[6].

〔표 2〕 FIPS 문서

표준화 문서	알고리즘
FIPS 203	CRYSTALS-Kyber → **ML-KEM** (Module-Latticed-Based Key-Encapsulation Mechanism)
FIPS 204	CRYSTALS-Dilithium → **ML-DSA** (Module-Latticed-Based Digital Signature Algorithm)
FIPS 205	SPHINCS+ → **SLH-DSA** (Statelss-Hash-Based Digital Signature Algorithm)
FIPS 206 (예정)	Falcon → **FN-DSA** (Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm)

2.1.2. 전환 정책

미국은 국가 암호체계를 2035년까지 전환하는 것을 목표로 하며 관련한 중장기 계획을 구체화하며 단계적으로 추진하고 있다.

2022년 5월 백악관은 국가안보각서(NSM-10)[8]를 발표하여 양자정보과학(Quantum Information Science, QIS) 분야에서 미국의 주도권을 확보하고, 양자컴퓨터로 인한 국가 안보 및 경제적 위험을 완화하기 위한 정책 및 지침을 제시하였다. 이어 같은 해 11월, 백악관 산하 예산관리국(Office of Management and Budget, OMB)은 NSM-10을 구체화한 세부 지침서(M-23-02)를 공개하였다. 해당 지침서는 연방 기관들이 CRQC에 취약한 암호 시스템을 포함하는 정보 시스템 · 자산을 식별하고 중요도 및 우선순위에 따라 목록을 정리해 제출하도록 요구하며 이를 준수하기 위하여 취해야 할 구체적인 지침과 절차를 제시하고 있다[9].

2022년 12월 제정된 “양자 컴퓨팅 사이버 보안 준비법(Quantum Computing Cybersecurity Preparedness Act, H.R.7535)”에 따라 OMB는 15개월 이내에 연방 정보 시스템을 양자내성암호로 전환하기 위한 전략의 주요 요소를 설명하는 보고서를 의회에 제

출해야 했다. 이에 따라 OMB는 국가 사이버국장실(Office of the National Cyber Director, ONCD), 국토안보부(Department of Homeland Security, DHS) 산하 사이버보안 및 인프라 보안국(Cybersecurity and Infrastructure Security Agency, CISA)과 협력하여 2024년 7월 관련 보고서를 발행하였다. 해당 보고서에는 연방 정보 시스템의 양자내성암호 전환 전략과 전환에 필요한 예산 및 대략적인 규모, NIST 주도의 양자내성암호 표준 개발 관련 현황 및 일정 등이 포함되어 있다[10].

2024년 9월, CISA는 M-23-02의 지침을 이행하기 위해 전환 전략서를 발표하였는데, 해당 문서는 연방 민간 행정 기관(Federal Civilian Executive Branch, FCEB)이 CRQC에 대비해 암호화 자산을 평가하고, 자동화 도구(ACDI)와 기존 CDM 프로그램을 활용해 양자내성암호로 전환할 수 있도록 방안을 제시하고 있다. 또한 단기, 중장기 목표를 통해 양자내성암호 전환 완료를 위한 구체적인 로드맵을 제공한다[11].

NIST 산하 국가사이버안보센터(National Cybersecurity Center of Excellence, NCCoE)는 M- 23-02 지침을 기술적으로 지원하기 위해 특별출간물인 SP 1800-38 시리즈의 초안을 공개하였다. 해당 시리즈는 총 3개의 문서로 이뤄져 있으며 문서마다 프로젝트가 존재한다. 2023년 4월 공개된 SP 1800-38A 초안은 양자내성암호 전환의 필요성을 비롯한 전환에 대한 전반적인 개요를 다루고 있다[12]. SP 1800-38B 초안은 암호화 자산 탐지, 리스크 평가를 위한 도구, 방법론 등을 소개하며 실질적인 전환 절차를 제시한다[13]. SP 1800-38C는 TLS, SSH 등 주요 암호 시스템에 양자내성암호 통합을 목표로 상호 운용성과 성능 등을 테스트한 결과를 포함하고 있다[14].

2.1.3. 국가안보시스템의 양자내성암호 전환

국가 안보와 관련된 민감한 데이터를 보호하기 위해국가안보시스템은 FCEB의 시스템에 대한 양자내성암호 전환 관련 지침들과는 분리되어 별도의 계획과 절차를 따른다. NSM-10에 명시된 바에 따라 국가안보시스템은 NSA(National Security Agency)의 관리 대상으로 명시되어 있기 때문에 NSA가 국가안보시스템의 양자내성암호 전환을 주도적으로 이끌고 있다. 이에 NSA는 2022년 9월 CNSA 1.0을 업데이트한 CNSA 2.0을 공개하며, CRQC 위협에 대응할 수 있는 암호 알고리즘(NIST 표준 양자내성암호, LMS, XMSS)들을 추가하였다[15].

2.2. 유럽

유럽은 미국과 달리 독립적인 표준화 공모전을 개최하기보다는 NIST에서 선정된 표준화 알고리즘을 기반으로 전환 작업을 진행하고 있다. 유럽전기통신표준협회(European Telecommunications Standards Institute, ETSI)를 중심으로 양자내성암호 전환에 필요한 기술적 지원과 가이드라인 수립에 더 많은 자원을 투입하고 있으며, 국가 차원에서 알고리즘 평가 및 적용 전략도 병행하고 있다. 유럽의 양자내성암호 표준화 및 전환 동향에 대해서는 유럽의 다양한 나라, 연합 기구 중 가장 활발하게 진행 중인 ETSI와 독일을 대표로 살펴본다.

2.2.1. ETSI

유럽의 표준화 작업은 ETSI를 중심으로 이뤄지고 있다. 2017년 설립된 ETSI의 양자 안전 암호화(Quantum-Safe Cryptography, QSC) 워킹그룹에서 양자내성암호 관련 작업을 수행한다. QSC 워킹 그룹은 관련 작업의 일환으로 2020년 7월 기술 보고서(TR 103 619 v1.1.1)를 발행하였다. 이 보고서는 조직이 양자컴퓨터의 위협에도 완전한 안전성을 보장하는 암호 상태(Fully Quantum-Safe Cryptographic State, FQSCS)로 전환 하기 위한 4단계 과정을 제시한다. 이는 자산목록 작성 → 전환 계획 준비 → 전환 실행 → 검토 및 최적화의 순서로 구성되며, 3단계(전환 실행 단계)까지 달성하기 위한 구체적인 전략과 권장사항을 포함하고 있다[16].

또한, 2024년 4월 양자내성암호 전환을 지원하기 위한 가이드라인(TR QSC 0024)에서 기업이 기존 암호 시스템을 양자내성암호 시스템으로 전환할 때 따라야 할 단계적 접근 방식(11단계)을 제시하였다. 이때, 모든 자산을 한 번에 전환하는 것은 비현실적이라는 점을 고려해 일정 간격 동안 재실행하는 ‘반복적 접근 방식’을 권장하고 있다[17].

2.2.2. 독일

독일은 연방정보기술보안청(BSI)이 양자내성암호 전환을 주도적으로 지원하고 있다. BSI는 2020년 3월 처음으로 양자내성암호를 권장했으며, Frodo-KEM, Classic McEliece, ML-KEM을 포함한 양자내성암호 알고리즘의 ISO/IEC 표준화를 지원하고 있다. 2022년 10월, BSI의 제안에 따라 ISO/IEC JTC1/SC27/WG2 (암호 및 보안 메커니즘의 표준화를 담당하는 워킹 그룹)에서 양자내성암호 PKE/KEM의 ISO/IEC 표준화를 위한 프로젝트가 시작되었으며, 현재 3가지 암호에 대한 프로젝트가 진행 중이다[18].

2024년 2월 BSI는 선택한 암호화 메커니즘의 보안성을 평가하고, 장기적인 사용 방향성을 제공하기 위해 기술 가이드라인(TR-02102-2)을 발간하였다. 이 지침서는 다양한 양자내성암호 알고리즘의 구현 방법을 제안하며, 정부 · 민간 부문에서 이를 실질적으로 적용할 수 있는 전략도 포함하고 있다[19].

표준화 지원, 전환 관련 가이드 발간 외에도 BSI는 양자내성암호 전환을 위한 다양한 프로젝트를 진행하고 있다. 양자내성암호(SPHINCS+, ML-KEM, Classic McEliece, ML-DSA, XMSS 등)를 구현한 암호화 라이브러리 “Botan”을 개발하고, TLS 1.3 키 교환에 양자내성암호를 적용하는 작업을 수행하고 있다. 또한, 독일은 행정용 공공키 인프라(V-PKI)를 양자내성암호로 전환하는 프로젝트를 추진하며 국가적 보안 강화와 양자 컴퓨터 위협에 대비한 전환 작업을 적극적으로 진행하고 있다[20].

2.3. 일본

일본은 유럽과 마찬가지로 자체적인 표준화 공모전을 진행하지 않고, 전환 관련 가이드와 양자내성암호 상용화에 집중하고 있다. 일본의 양자내성암호 전환은 정보통신연구기구(National Institute of Infor- mation and Communications Technology, NICT)와 정보처리 추진기구(Informational tech- nology Promotion Agency, IPA)가 공동 운영하는 암호기술 연구 및 평가 위원회(Cryptography Research and Evaluation Committees, CRYPTREC)와 NICT가 주도하고 있다.

2.3.1. CRYPTREC

CRYPTREC은 암호화 기술의 안정성 및 효율성을 평가하고 공공·민간 부문에서 사용할 암호 기술의 표준을 제공하기 위해 설립된 기관이다. 이 기관은 새로운 암호 기술의 평가와 추천 목록을 작성하며, 일본 공공기관 및 민간 부문에서 사용할 암호화 기술에 대한 지침을 제공하는 역할을 맡고 있다.

2023년 4월, CRYPTREC의 암호기술 평가위원회에서 발간한 암호 기술 가이드는 양자내성암호의 필요성과 용도별 전환 전략, 국내·외 표준화 및 연구 동향, 주요 알고리즘에 대한 상세 설명 등을 다루고 있다[21]. 또한, 2023년에는 양자내성암호 전환을 위해 구성된 암호기술 조사 워킹그룹이 전환 관련한 연구를 활발하게 진행하였다. 암호기술 평가위원회 워킹그룹은 2022년에 작성된 암호기술 가이드[21]의 개정을 위해 연구 및 가이드 작성 방향을 논의하였다[22]. 2024년 7월에 발간한 보고서에 따르면 현재 가이드 개정이 진행 중인 것으로 추정된다.

2.3.2. NICT

NICT는 양자내성암호 알고리즘 구현 및 응용 기술 연구, 민간 기업과의 협력을 통한 양자내성암호 상용화 지원 업무를 담당하고 있다.

NICT는 이러한 노력의 일환으로 2024년 10월 민간 기업과 함께 개발한, 양자내성암호(ML-DSA) 탑재 스마트 카드 시스템 SecureBridge™를 공개했다. 이 시스템은 2022년 10월 공개했던 스마트카드(PQC CARD®)의 업그레이드 버전으로, 기존 공개키 암호(ECDSA)와 양자내성암호를 동시에 지원하는 하이브리드 인증서를 도입하여 시스템 호환성을 확보하였다. 추가로 SecureBridge는 의료 데이터 지원 시스템인 'H-LINCOS'에 파일럿 테스트를 진행하여 다양한 전환 단계의 시스템에서 정확한 사용자 인증과 데이터 탐색이 가능함을 입증했다. 이를 기반으로 2025년에 고수준의 보안이 필요한 의료·금융 분야에 제한적으로 적용하고, 2030년까지 본 서비스를 상용화할 계획이라고 알려져 있다[23].

2.4. 중국

중국은 중국암호학회(Center for Advanced China Research, CACR)를 주축으로 2018년 6월 양자내성암호 알고리즘 발굴을 위해 국가 공모전을 개최하였다[24]. 해당 공모전은 총 38개의 알고리즘을 평가한 뒤 2020년 1월 종료되었으며, 이 중 14개의 알고리즘이 선정되었다. LAC.PKE 알고리즘을 포함하여 3개의 암호 알고리즘이 1등으로 선정되었고, 선정된 14개의 알고리즘 중 11개가 격자 기반 암호 알고리즘으로 구성되었다[25].

중국의 양자내성암호 전환 관련 정책은 미국, 유럽과 달리 공식적인 문서로 공개되지 않고 있으며, 국가 공모전 이후의 행보 역시 제한적으로 드러나고 있다. 다만, 중국의 연구 및 정책적 흐름을 살펴보면, 양자내성암호보다는 양자키분배와 같은 양자통신 기술에 더 큰 비중을 두고 있는 것으로 보인다. 특히, 13차 산업혁명 기간(2016~2020년)부터 14차 5개년 계획 기간(2021~2025)까지 모두 양자 통신 개발을 정책적으로 지원하고, 그에 따른 다양한 성과를 거둔 점이 이를 뒷받침한다[26]. 이러한 행보는 양자컴퓨터의 보안 위협에 대응하는 중국의 전략적 우선순위가 다른 국가들과 차별화되어 있음을 시사한다.

Ⅲ. 국내 양자내성암호 표준화·전환 정책 동향

본 장에서는 한국의 양자내성암호 표준화 동향과 전환 정책 동향에 대해서 살펴본다.

3.1. 표준화

한국은 미국, 중국에 이어 2021년 11월 양자내성암호 공모전을 개최하였다. 이 공모전은 KpqC연구단(산·학·연·관의 암호 관련 전문가들로 구성)이 주축이 되어 진행되었다. 공모전 초기에 16개의 알고리즘으로 시작하여 1라운드 평가 결과 8개의 알고리즘이 2라운드에 진출하였다('23년 12월). 각 알고리즘은 안전성, 효율성, 다양한 환경에서의 활용성 등의 항목을 기준으로 평가되었으며, 2라운드에 진출한 알고리즘은 [표 3]에서 확인할 수 있다[27].

〔표 3〕 KpqC 공모전 2라운드 진출 알고리즘

종류	기반 문제	알고리즘
PKE/KEM	격자 (Lattice)	NTRU+
		SMAUG-T
	코드 (Code)	PALOMA
		REDOG
전자서명	영지식 (Zero-Knowledge Proof)	AIMer
	격자 (Lattice)	HAETAE
		NCC-Sign
	다변수 (Multivariate)	MQ-Sign

3.2. 전환 정책

2023년 7월, 국가정보원과 과학기술정보통신부는 행정안전부, 한국인터넷진흥원, 국가보안기술연구소 등 관계 부처와 협력하여 기존 공개키 암호체계를 양자내성암호로 전환하기 위한 종합 대책인 "汎국가 양자내성암호 전환 마스터플랜"을 수립하였다. 이 마스터플랜은 양자내성암호 전환 추진 전략, 향후 계획, 전환 로드맵을 포함하고 있다.

마스터플랜에 따르면 추진 전략은 크게 ① 역량 확보 및 제도·절차 마련과 ② 전환 지원 및 기반·생태계 조성으로 구성되어 있다. 전략별 과제는 [표 4]에 정리

〔표 4〕 양자내성암호 전환 마스터플랜 전략별 과제

전략	과제
① 역량 확보 및 제도·절차 마련	**기술 확보** : KpqC 개발, 표준화, 취약암호탐지·검증기술·전환 응용 기술 확보
	제도 정비 : 보안강도 재정립, 암호사용 기준(안내서) 제시, KCMVP(암호모듈 검증제도) 정비
	절차 정립 :액션플랜(세부 시행내용) 수립, 전환 추진단 설립, 전환 식별 기준 정립
② 전환 지원 및 기반·생태계 조성	**암호체계 전환 지원** : 전환 실증사업, 전환 가이드 개발, 테스트베드·지원센터 구축
	인증 인프라 고도화 : PKI 관련 협력 체계 구축, 단계별 이행 기반 마련
	산업기반 구축 : 중장기 인력 양성 대책 마련, 특성화 기업 육성 지원, 대국민 인식 제고

되어 있다.

전환 로드맵에 따르면, 2030년까지 양자내성암호 전환을 위한 제도적 기반을 구축하고, 2035년까지 전환을 위한 기술 및 정책적 지원 체계 구축, 안전한 암호체계 구현 등을 목표로 하고 있다[28]. 추가적으로 마스터플랜의 절차 정립 과제 중 하나인 액션플랜 수립이 진행 중이다.

Ⅳ. 결 론

본 논문에서는 미국, 유럽, 중국, 일본 그리고 한국의 양자내성암호 전환과 관련된 표준화 및 정책 동향을 비교 · 분석하였다. 특히, 미국은 NIST 표준화 과정과 연계된 강력한 정책 프레임워크(NSM-10, M-23-02)를 통해 양자내성암호 전환의 선두 주자로 자리하고 있다. 미국의 전환 계획은 세부적인 로드맵과 법적 지원에 기반해 순조롭게 진행 중이며, 2025년에도 주요 지침에 따라 무리 없이 진행될 것으로 예상된다. 미국의 사례는 양자내성암호 전환이 체계적인 정책 및 법률적 기반 아래 효과적으로 수행될 수 있음을 보여준다.

한국은 2023년 양자내성암호 전환 마스터플랜을 발표하며 체계적인 전환 작업의 첫발을 내디뎠다. 성공적인 전환을 위해 한국은 주요국의 사례를 참고하고, 마스터플랜의 세부 계획을 신속히 수립해야 한다. 또한, 각 관계 부처 간 긴밀한 협력을 통해 단계별 전환 작업을 차질 없이 진행할 수 있도록 지원 체계를 강화해야 한다. 이러한 노력을 지속적으로 기울인다면 2035년까지 양자내성암호 전환 목표를 성공적으로 달성할 수 있을 것으로 기대된다.

참 고 문 헌

[1] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Rev.* 41, pp.303-332, 1999.

[2] M. Mosca, M. Piani, “Quantum Threat Timeline Report 2023 Executive Summary,” *Global Risk Institute*, Jan 2024.

[3] 유다은, 김준섭, 김기문, “국내·외 양자내성암호 전환 정책 및 상용화 동향,” vol. 33, no. 1, pp. 59-63, 2023.

[4] G. Alagic, et al., “Status report on the third round of the NIST post-quantum cryptography standardization process,” *NISTIR,* 8413, July 2022.

[5] SIKE teams, “SIKE Foreword and post- script,” Aug 2023.

[6] NIST, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards, Aug 2024.

[7] G. Alagic, et al., “Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process,” *NISTIR,* 8528, Oct 2024.

[8] The White House, “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,” May 2022.

[9] OMB, “Migrating to Post-Quantum Cryptography,” Nov 2022.

[10] OMB, “REPORT ON POST-QUANTUM CRYPTOGRAPHY,” July 2024.

[11] CISA, “Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools”, Sep 2024.

[12] NCCoE, “Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography(draft)”, *NIST Special publication 1800-38A*, Apr 2023.

[13] NCCoE, “Quantum Readiness: Cryptographic Discovery(draft)”, *NIST Special publication 1800-38B*, Dec 2023.

[14] NCCoE, “Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards(draft)”, *NIST Special publication 1800-38C*, Dec 2023.

[15] NSA, “Announcing the Commercial National Security Algorithm Suite 2.0,” Sep 2022.

[16] ETSI, “Migration strategies and recommendations to Quantum Safe schemes,” July 2020.

[17] ETSI, “A Repeatable Framework for Quantum-Safe Migrations,” April 2024.
[18] BMBF, “Handlungskonzept Quantentechnologien,” April 2023.
[19] BSI, “Cryptographic Mechanisms Recommednations and Key Lengths,” Feb 2024.
[20] ETSI, “BSI Post-Quantum Update,” *Security Conference 2024*, Oct 2024.
[21] CRYPTREC, “暗号技術ガイドライン(耐量子計算機暗号),” April 2023.
[22] CRYPTREC, “CRYPTREC Report 2023 Cryptographic Technology Evaluation Committee Report,” pp. 31-36, July 2024.
[23] NICT, https://www.nict.go.jp/en/press/2024/10/07-1.html, Oct 2024.
[24] CACR, https://sfjs.cacrnet.org.cn/site/content/309.html, Jun 2018.
[25] CACR, https://www.cacrnet.org.cn/site/content/854.html, Jan 2020.
[26] yalejournal, https://www.yalejournal.org/publications/chinas-quantum-ambitions, Feb 2024.
[27] 양자내성암호연구단, “https://kpqc.or.kr/competition_02.html,” 2024년 11월.
[28] 관계부처, “汎국가 양자내성암호 전환 마스터플랜,” 2023년 7월.

〈저자소개〉

양 유 진 (Yu Jin Yang)
2022년 2월 : 한성대학교 IT융합공학부 졸업
2024년 2월 : 한성대학교 IT융합공학과 석사
2024년 5월~현재 : 한국인터넷진흥원 차세대암호 기술팀 주임연구원
<관심분야> 정보보호, 암호알고리즘, 양자내성암호 등

송 강 수 (Kang Soo Song)
2004년 2월 : 충남대학교 전산학 석사
2019년 3월 : 숭실대학교 공학박사 수료
2007년 4월~현재 : 한국인터넷진흥원 차세대암호기술팀
<관심분야> 머신러닝, 사물인터넷, 양자내성암호

손 기 종 (Ki Jong Son)
2014년 3월~현재 : 한국인터넷진흥원 차세대암호기술팀 팀장
<관심분야> 소프트웨어 취약점 분석, 인공지능, 암호 등