양자내성암호로의 마이그레이션 연구 및 정책 동향

송경주*, 권혁동*, 심민주*, 이민우*, 서화정**

*한성대학교 (대학원생)

**한성대학교 (교수)

Research and Policy Trends on Migration to Post-Quantum Cryptography

Gyeong-Ju Song* Hyeok-Dong Kwon* Min-Joo Sim* Min-Woo Lee* Hwa-Jeong Seo**

*Hansung University(Graduate student)

**Hansung University(Professor)

요 약

본 논문에서는 기존 암호시스템을 양자내성암호로 마이그레이션 하기 위한 연구 및 정책 동향을 살펴보았다. 현재 사용하는 암호는 양자컴퓨터는 미래 대규모 양자컴퓨터가 등장하면 보안성 모호할 것이라 예상되며 빠른 시일 내에 양자내성암호로의 전환을 권고하고 있다. 기존 암호화 시스템을 양자내성암호로 전환하기 위해서는 필요한 절차가 있는데, 각 국가에서는 이에 대한 로드맵 및 정책을 제공하여 전환에 대한 가이드라인을 제공하고 있다. 본 논문에서는 그 중 미국 및 유럽을 중심으로 마이그레이션 전환 연구 및 정책을 살펴본다.

I. 서론

미래 대규모 양자컴퓨터의 등장은 기존 공개키 암호의 보안성을 깨뜨릴 것이라 예상하며[1] 이에 대응하기 위해 National Institute of Standards and Technology(NIST)는 2017년 초 양자 저항을 가진 양자 내성 암호(PQC, Post-Quantum Cryptography) 체계 확립을 위한 공모전을 진행하였다. 해당 공모전은 미래 공개키 암호 해독 위험에 대비하기 위해 다양한 환경 및 유형에서 안전성과 효율성을 가진 PQC 표준 후보군을 제정하였다. 그 결과 2022년 PKE/KEMs 1개, DSA 3개 표준으로 선정되었다: CRYSTALS-KYBER(격자기반PKE/KEMs), CRYSTALS-KYBER(격자기반 DSA), FALCON(격자기반 DSA), SPHINCS+(해시기반 DSA)[2].

현재 암호화된 자산들을 보호하기 위해서는 기존 암호에 대한 PQC 전환이 필요하다고 여겨지며 이에 따라 현재 사용되는 암호 시스템을 post-quantum 암호로 전환하여 양자컴퓨터로부터 보호하기 위한 정책 및 연구가 진행되고 있다.

본 논문에서는 기존 암호시스템을 안전하게 양자내성암호로 마이그레이션 하기 위한 연구 및 정책 동향을 살펴본다.

II. 연구동향

미국, 유럽 등 각 나라들은 기존 암호를 양자내성 암호로 마이그레이션 하기 위한 전략 및 지침서를 제공하여 기업 등에 효율적인 방향을 제공하고자 노력하고 있다. <표 1>, <표 2>는 미국 및 유럽에서 발표한 양자 내성 암호 전환관련 지침 및 절차를 보여준다. 각 나라에서는 꾸준히 마이그레이션 전환을 권고하며 전환을 위한 절차 로드맵을 제공하여 방법을 제시한다. 본 논문에서는 그 중 ETSI, NIST, NCCoE, 미국 국토안보부, ANNSSI의 4가지 마이그레이션 보고서에 대해 자세히 살펴본다.

표 1. 양자내성 암호 전환 관련 전환 정책 및 절차(미국)

발간 년도	Tittle	발간 기관
2020.08	Towards PQC Standardization and Migration [3]	NIST
2020.10	Considerations in Migrating to Post-Quantum	NIST
2021.04	Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms [4]	NIST
2021.08	Migration To Post-Quantum Cryptography [5]	NIST NCCoE
2021.09	Preparing for Post-Quantum Cryptography [6]	국토안보부
2021.10	Migration to Post-Quantum Cryptography	NIST
2022.05	취약한 암호시스템 위험 완화 및 양자컴퓨팅에서 미국의 리더십 진흥을 위한 국가. 보안각서(NSM 10)	백악관
2022.08	Preparing Critical Infrastructure for Post-Quantum Cryptography [7]	국토안보부, CISA
2022.11	Migrating to Post-Quantum Cryptography [8]	백안관

표 2. 양자내성 암호 전환 관련 전환 정책 및 절차(유럽)

발간 년도	Tittle	발간 기관
2017.02	Quantum Safe Cryptography; Case Studies and Deployment Scenarios [9]	ETSI (유럽)
2020.07	Migration strategies and recommendations to Quantum Safe schemes [10]	ETSI (유럽)
2022.03	ANSSI views on the Post-Quantum Cryptography transition [11]	ANSSI (프랑스)

3.1 Migration strategies and recommendations to Quantum Safe schemes (ETSI)

2020년 European Telecommunications Standards Institute (ETSI)는 Non-quantum safe 한 상태에서 Fully Quantum-Safe Cryptography(FQCS) 환경으로 마이그레이션 하는 문제에 관한 보고서를 발표하였다. 해당 보고서는 Quantum-safe 마이그레이션 과정을 크게 3단계로 분류하였다. 1단계: 시스템 편집에서는 시스템에서 사용되는 암호화 자산(HW/SW) 및 프로세스 식별을 진행한다. 2단계: 마이그레이션 준비 단계에서는 자산 전체 목록 및 자산에 대한 정보를 포함하며, Hardware Based Security Environment (HBSE)을 먼저 마이그레이션 한 뒤, HBSE에 종속된 자산을 마이그레이션 해야 한다고 권장한다. 경제적으로 기존 암호화 자산을 quantum-safe 상태로 마이그레이션 하는 것이 불가능할 경우 non-QSC 리소스를 격리하는 단계를 포함해야 한다. 마이그레이션 되지 않은 non-QSC 자산은 물리적으로 격리되며 해당 내부에서 관리된다. 3단계: 마이그레이션 실행에서는 마이그레이션 계획에 대한 실행 가능성을 판단하기 위해 마이그레이션을 시뮬레이션하고 테스트를 수행한다.

3.2 Migration strategies and recommendations to Quantum Safe schemes (NIST, NCCoE)

2021년 1월 NIST, NCCoE는 Post-quantum 마이그레이션 계획을 발표하였다. NIST에서는 해당 작업을 위해 quantum-resistant 공개키 암호 표준화 작업을 진행하였으며 NCCoE는 지속적인 보안을 위한 post-quantum 마이그레이션 논의를 진행하였다. 현재 post-quantum 암호 전환 가속화를 위한 애플리케이션에 대한 표준, 지침, 규정, 하드웨어, 펌웨어, 운영 체제, 통신에 대한가이드 시스템이 없다. 따라서 해당 보고서에서는 quantum-resistant 암호화 업데이트가 필요한 위치를 신속히 발견하기 위한 계획을 제시하고 전환 단계를 작성하였다. Quantum-safe로 전환하기 위해서는 암호화되는 정보 및 엑세스 관리 프로세스의 암호화 키 설정, 사용 HW/SW, 라이브러리, 임베디드 코드 등을 식별해야하며 과정은 크게 3단계로 진행된다. 초기 단계에서는 사용되는 하드웨어, 펌웨어, 운영체제, 통신 프로토콜, 암호화 라이브러리 등

에서 암호화 사용 위치 및 방법을 식별하는 자동화 도구 개발을 진행한다. 중간단계는 “Mosca’s Theorem” 및 위험 관리 방법론을 사용하여 식별된 공개키 암호화 구성 요소 및 관련 자산에 대한 마이그레이션 우선순위를 지정한다. 최종단계에서는 다양한 유형의 자산들을 quantum-resistant 알고리즘으로 마이그레이션 하는 기술을 지원하기위한 체계적인 접근 방식을 제공한다.

3.3 Preparing for Post-Quantum Cryptography (미국 국토안보부)

2021년 9월 미국 국토안보부(DHS)는 NIST와 협력하여 양자 컴퓨팅 기술로부터 데이터 및 시스템을 보호하고 관련 위험을 줄이는데 도움이 되는 로드맵을 발표하였다. 해당 보고서에서 제안한 로드맵은 <표 3>과 같다.

표 3. 미국 국토안보부의 PQC 마이그레이션 전환 계획 로드맵

Roadmap	
1	관련 알고리즘 및 프로토콜 개발을 위한 참여 증진
2	1) 중요 데이터 셋 목록 작성 2) 위험 데이터 식별 3) 양자 컴퓨터 사용 시 해독되는 데이터 식별
3	암호화 기술을 모든 기능에 사용하는 시스템 수행
4	Post-quantum 요구 사항을 위한 보안 표준식별
5	공개 키 암호화 사용 위치 및 목적 식별
6	요소들을 고려하여 암호화 전환을 위한 우선순위 지정
7	Post-quantum 암호화 표준 발표 시, 시스템 전환 계획 전환 계획 수립을 위한 지침 제공

3.4 ANNSSI views on the Post-Quantum Cryptography transition

2022년 3월 프랑스 ANNSSI는 문서를 통해 post-quantum 전환 관점을 작성하였다. 해당 문서를 통해 NIST 표준으로 선정된 PQC 알고리즘에 대한 maturity level을 과대평가 하지 말아야 한다는 의견을 발표하였다. 선정된 PQC가 아직 암호분석 후견이 부족하며 표준이 발표된 이후에도 프로토콜 체계 통합, 보안 구현 설계 등의 연구가 지속적으로 필요할 것이라 보고 있다. 따라서 PQC의 immaturity를 인정하되 PQC의 immaturity로 인해 첫 PQC 배포가 연기되어선 안된다고 언급한다. ANSSI는 PQC 알고리즘 및 구현에 대한 신뢰를 높이기 위해 모든 산업에서 2022년 4월에 점진적으로 오버랜 전환을 시작하도록 권장하며 pre-quantum에 관한 보안 회귀를 방지할 것을 권장하였다. <그림 1>은 ANSSI에서 권장하는 단계에 따른 점진적 post-quantum 전환 로드맵을 보여준다.

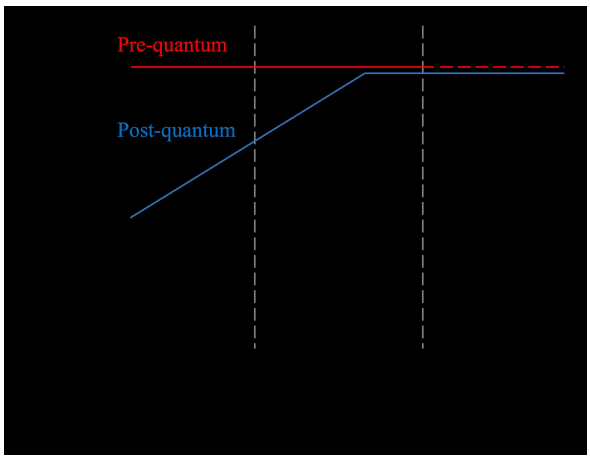

그림 1 단계에 따른 ANSSI 권장 점진적 Post-quantum 암호 마이그레이션 로드맵

Phase 1(현재)는 Hybridation을 통해 pre-quantum 보안에 추가적인 post-quantum 보안을 제공한다. 최초 배포에 FrodoKEM, Kyber, Dilithium 등이 적합할 것으로 판단되며 NIST 표준화 알고리즘의 선택이 필수 조건은 아니다. Phase 2 (2025년 이후)는 Hybridation을 통해 pre-quantum 보안에 대한 회귀를 피하고 post-quantum 보안을 제공해야 한다. 이때, post-quantum 공개키 알고리즘은 하이브리드 매커니즘 내부에서 계속 포함되어야 한다. 만약 Long-term 보안이 필요할 경우 post-quantum

이 필수적일 수 있다. Phase 3 (2030년 이후)은 독립적인 post-quantum 암호화를 선택적으로 도입한다. post-quantum 보안 수준은 현재 pre-quantum 보안 수준과 동일할 것으로 예상하며 일부 post-quantum 암호 알고리즘은 하이브리드 없이 사용 가능해야한다.

III. 결론

본 논문에서는 기존 암호 시스템을 양자내성암호로 마이그레이션 하기 위한 연구 및 정책 동향에 대해 살펴보았다. 각 국가들은 대규모 양자컴퓨터에 안전하게 대비하기 위해 기존 암호 시스템을 post-quantum 암호화로 전환을 권고하며 이를 위한 단계별 지침서 및 로드맵을 제공하여 기업 등에 효율적인 마이그레이션 방향을 제공하고자 노력하고 있다.

IV. Acknowledgement

This work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%) and this work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 50%).

[참고문헌]

[1] Shor, P. W. "Algorithms for quantum computation: discrete logarithms and factoring", In proceedings 35th annual symposiumon foundations of computer science, pp. 124-134.

[2] NIST, "Selected Algorithms 2022", 2022, https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[3] NIST, “Towards PQC Standardization and Migration” https://icmconference.org/wp-content/uploads/Pre-ICMC-Chen-08122020-.pdf

[4] NIST, “Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms”, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

[5] NCCoE, NIST “Migration To Post-Quantum Cryptography”, https://www.nccoe.nist.gov/sites/default/files/legacy-files/pqc-migration-project-description-final.pdf

[6] 미국 국토안보부, “Preparing for Post-Quantum Cryptography”, https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf

[7], CISA, “Preparing Critical Infrastructure for Post-Quantum Cryptography”, https://www.cisa.gov/news-events/alerts/2022/08/24/preparing-critical-infrastructure-post-quantum-cryptography

[8] 백악관, “Migrating to Post-Quantum Cryptography”, https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

[9] ETSI, “Quantum Safe Cryptography; Case Studies and Deployment Scenarios”,

https://www.etsi.org/deliver/etsi_gr/qsc/001_099/003/01.01.01_60/gr_qsc003v010101p.pdf

[10] ETSI, “Migration strategies and recommendations to Quantum Safe schemes”, https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[11] ANSSI, “ANSSI views on the Post-Quantum Cryptography transition”, https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/