정 보 보 호 학 회 지
제 33 권 제1호, 2023. 2

국내·외 양자내성암호 전환 정책 및 상용화 동향

유 다 은*, 김 준 섭**, 김 기 문***

요 약

양자컴퓨터의 등장으로 기존 암호체계의 붕괴 위협이 가시화 되면서 이에 대한 대책 마련이 필요한 시점이다. 미국 등 세계 주요 국가들은 양자컴퓨터로도 해독하기 어려운 양자내성암호를 연구하고 암호체계 전환을 준비하고 있다. 이 논문에서는 국내·외 양자내성암호 전환 계획, 추진 전략 등을 살펴보며, 산업계에서의 양자내성암호 적용 사례 등의 양자내성암호 전환 관련 동향을 알아보고자 한다.

Ⅰ. 서 론

2019년 10월 네이처 학술지는 구글이 개발한 양자컴퓨터가 현존하는 슈퍼컴퓨터의 한계를 뛰어넘는 양자우위(qunatum supremacy)를 달성했다고 밝혔다.[1] 양자 컴퓨터는 기존의 컴퓨터가 0과 1의 비트로 처리하는 것과 다르게 0과 1을 동시에 갖는 큐비트 단위로 연산을 처리한다. 그렇기 때문에 정보처리와 연산 속도가 지수 함수적으로 증가하여 빠른 속도로 문제해결이 가능해 복잡한 계산과 대량 데이터 처리에 강점을 지닌다. 양자컴퓨터의 등장은 Shor 알고리즘으로 기존의 RSA와 같은 인수분해 문제의 복잡도에 의존하는 암호체계를 해독할 수 있는 위협이며, 산업 全분야의 ICT 환경에서 사용하고 있는 공개키 암호가 더 이상 공개키 암호는 사용이 불가능 한 것을 의미한다.[2] 결국, 양자환경에서의 보안 위협에 대응하기 위해 양자내성암호(Post Quantum Cryptograpyh, PQC) 도입이 필요하며 본 논문에서는 주요 국가들의 양자내성암호 전환 동향을 파악하고자 한다.

Ⅱ. 양자내성암호 전환 동향

본 장에서는 주요 국가들의 양자컴퓨터 공격에 취약한 기존 공개키 암호를 대체하기 위해 해결 불가능한 다양한 수학적 난제에 기반한 안전성을 갖는 양자내성암호로의 전환 관련 정책 동향을 살펴보고자 한다.

2.1. 양자내성암호 전환 동향(미국)

양자내성암호 전환을 주도하고 있는 국가는 미국이다. 미국은 16년부터 전환을 준비해 알고리즘 표준화, 시나리오, 로드맵 등을 제시했으며 '22년 9월 국가 안보시스템 적용 알고리즘 목록에 기존에 포함되어 있던 인수분해, 이산로그 기반의 알고리즘을 제외하고 양자내성암호 알고리즘을 포함하였다.

2.1.1. 표준화

국립표준연구소(NIST)에서는 16년도부터 양자내성암호 알고리즘 공모전을 추진하고 표준화 작업을 진행하고 있다. 1, 2, 3라운드를 거쳐 현재('22년 7월)까지 격자기반 알고리즘 3종, 해시기반 알고리즘 1종 선정하였으며, 격자 기반 알고리즘의 의존도 해소를 위하여 추가 선정 대상 4라운드 후보와 전자서명 알고리즘 추가 공모를 공지했다.[3]

〔표 1〕 NIST, 양자내성암호 알고리즘 표준화

암호기능	알고리즘	비고
키교환/공개키 암호화	BIKE (코드 기반)	4라운드 후보
	Classic McEliece (코드 기반)	
	HQC (코드 기반)	

* 한국인터넷진흥원 차세대암호기술팀 (선임연구원, deyoo@kisa.or.kr)
** 한국인터넷진흥원 차세대암호기술팀 (책임연구원, jskim@kisa.or.kr)
*** 한국인터넷진흥원 차세대암호기술팀 (팀장, kkm@kisa.or.kr)

암호기능	알고리즘	비고
키교환/공개키 암호화	SIKE (아이소제니 기반, 안전하지 않음)	4라운드 후보
	Kyber (격자 기반)	표준화 대상 알고리즘
전자서명	Dilithium (격자 기반)	
	FALCON (격자 기반)	
	SPHINCS+ (해시기반)	

2.1.2. 양자내성암호 전환 시나리오

국립표준연구소(NIST)의 국가사이버안보센터(NCCoE)는 ’21년 6월 양자내성암호 전환 시 고려사항과 절차를 설명한 시나리오를 발표했다. NIST에서는 FIPS-140 검증받은 하드웨어 및 소프트웨어, 암호 라이브러리, 응용프로그램, 운영체제, 산업계에 사용중인 자체 통신 프로토콜 5가지 암호제품 유형별 대체 · 시나리오를 제시했다. 대부분의 시나리오에서 공통적으로 공개키 암호 식별, 우선순위 선별, 적절한 양자내성암호 알고리즘을 선택하는 내용이 포함되어 있다.[4]

2.1.3. 양자내성암호 전환 로드맵

미국 국토안보부(DHS)는 ’21년 10월 표준화와 연계하여 실용적인 전환 방안과 대책 등을 논의하기 위한 암호전환 워크샵 추진을 시작으로 ’21년 10월 양자내성암호 전환 로드맵을 발표했다. 로드맵은 2030년까지 자산데이터 식별 및 시스템 우선순위 설정(~‘23),알고리즘 표준 발표(‘24), 양자내성암호표준으로 시스템 전환(~‘30) 순으로 목표했으며 양자내성암호로의 전환에 필요한 조치사항에 대한 가이드[표 2]를 제공했다.[5]

〔표 2〕 DHS, 양자내성암호 전환준비 절차

순서	전환단계	내용
1	양자내성암호 표준개발기구와의 교류 강화	기관의 CIO는 필요한 알고리즘 및 관련 프로토콜 변경사항과 관련한 표준 개발 조직과의 협력을 강화해야 함
2	핵심데이터 목록 관리	이 정보를 통해 현 단계에서 향후 위험한 데이터를 식별하고,
2	핵심데이터 목록 관리	암호학적으로 양자 컴퓨터를 사용할 수 있게 되면 해독이 될 수 있는 사항을 식별 할 수 있음
3	암호기술 목록관리	기관은 향후 원활한 전환을 촉진하기 위해 암호기술을 사용하는 모든 시스템을 식별 나열해야 함
4	내부 표준 식별	기관내 사이버보안 담당관은 향후 양자내성 요구사항을 반영하여 업데이트가 필요한 ″획득, 사이버보안 및 데이터 보안 표준″을 식별해야 함
5	공개키암호 식별	기관은 앞에서 식별된 데이터, 시스템, 암호기술에서 공개키암호가 사용되는 위치와 사용목적을 식별하여 해당시스템을 ″양자 취약″으로 표시해야 함
6	교체대상 시스템 우선순위 지정	기관의 역할, 목표 및 요구사항에 따라 암호 전환을 위해 시스템의 우선순위를 정할 수 있음. 기관은 양자 취약 시스템을 평가할 때, 아래 사항을 고려해서 우선순위 지정

2.1.4. 바이든, 행정명령 및 국가안보각서 서명

’22년 5월 미국 바이든 대통령은 양자정보과학 분야 국가 경쟁력 강화를 위한 행정명령과 국가안보각서에 서명해 양자내성암호 기술로의 전환을 촉진하였다. ‘국가 양자 이니셔티브(National Quantum Initiative) 자문위원회 강화를 위한 행정명령’[6]은 양자컴퓨팅 기술 분야의 다양한 전문가와 이해관계자로 구성된 대통령 직속 자문위원회를 설치하며, ‘양자컴퓨팅에

〔표 3〕 양자컴퓨터 위험을 완화하기 위한 각서 주요 내용

기간	수행 내용
~ ‘22. 8. 2	· 국가사이버안보센터 내 양자내성암호 전환 프로젝트 설립
~‘ 22. 10. 31	· 현재 사용 중인 모든 암호화 시스템 목록 작성 요건 수립(우선순위 핵심 IT 자산 목록, 양자내성암호 전환 평가 프로세스 필수 포함)
~ ‘23. 10. 18	· 양자 취약성 제거를 위해 수립된 일정 공개 · NIST 표준 공개 이후 암호화 시스템을 양자내성암호로 전환하는 계획을 수립하는 것을 의무화하는 각서 교부
~23. 12. 31	· 미국의 양자컴퓨팅 지적재산권, 연구개발 및 기타 민감한 기술 보호 증 관련위협에 대응하기 위한 계획 수립 요구 · 양자내성암호 키 교환을 추가로 보호하기 위한 솔루션 실행

서 미국의 주도권 증진 및 취약한 암호 시스템 위험 완화를 위한 국가안보각서[표 3][7]'는 양자정보과학에서 미국의 경쟁력을 강화하고, 양자내성암호로의 전환이 필요한 IT 시스템의 목록을 상세히 작성하도록 제시하고 있다.

2.2. 양자내성암호 전환 동향(유럽)

유럽에서도 양자내성암호 전환을 위해 표준화, 시나리오를 제시하는 등 30년 이후의 양자내성암호 사용을 위한 계획을 마련해 발표했다.

2.2.1. ETSI, 양자내성암호 전환 표준화 및 시나리오

유럽 표준기구인 ETSI에서는 양자내성암호 알고리즘의 전반적인 구성요소를 정의하고 표준화하기 위한 프레임워크를 개발('16년 7월) 하였으며[8] '20년 7월에는 기업 또는 기관 등 개별 조직에서 양자내성암호로의 전환을 추진하기 위해서 필요한 절차를 규정한 문서인 양자내성암호 전환 전략 및 요구사항 문서[9]를 발간했다. 이 문서에서는 전환하기 위해 자산목록 구축, 전환계획 수립, 전환 실행을 제시하였다. 1단계 자산목록 구축 단계에서는 시스템에 있는 암호자산과 프로세스를 파악하는 것으로 인프라에 대한 의존성을 파악해야 한다. 또한 조직에서는 관리자 임명, 예산 할당 등의 사항을 지원해야 한다. 2단계 전환계획 수립 단계에서는 1단계에서 구축한 자산이 전환해야 하는 지 여부, 순서, 종속성 테스트를 포함한 시험, 상호호환성 등을 고려해야 하며, 전환 과정에서도 자산이 보호될 수 있도록 전환 계획을 수립해야 한다. 이러한 과정에서 조직은 전환 책임자 지정, 예산 할당, 다운타임 관리를 지원해야 한다. 마지막 3단계인 전환 실행 단계에서는 1단계의 자산에 대해 2단계의 계획을 구현하는 것으로 전환 과정을 추적하고 측정하는 위험 관리를 해야 한다. 위험 관리에서는 사전 시뮬레이션 및 테스트를 수행함으로써 소요되는 비용 등을 추정하고 실행 성공 가능성을 높일 수 있다.

2.2.2. 프랑스, 양자내성암호로의 전환을 위한 계획 발표

프랑스 사이버안보국(ANSSI)은 '22년 1월 양자내성암호 전환을 위한 계획을 발표했으며, 주요 내용으로 1단계에서는 안전성 추가개념으로 하이브리드 방식의 양자내성 암호를 도입, 2단계 '25년 이후에는 확실한 양자내성체계를 구축하기 위해 하이브리드 방식으로 모든 영역에 양자내성암호 도입, 3단계 '30년 이후에는 양자내성암호 단독 사용을 계획하고 있다[10].

2.2.3. 세계경제포럼(WEF), 양자안전 전환의 프레임워크 제시

세계경제포럼(WEF)에서는 양자 컴퓨터 기술 발전으로 인한 보안 위협으로부터 사이버 시스템과 디지털 경제를 안전하게 보호하기 위해 양자 보안 시스템으로 전환을 추진하고자 조직이 자체적으로 양자 리스크를 파악하고 각자의 기술적 환경 등을 고려한 양자 안전 전환의 프레임워크를[표 4] 제시했다. 또한 일반 기업과 이사진, 사이버 기업, 정책 입안자의 관점에서 전환을 추진하는 과정에서의 고려사항을 제시하였으며 특히, 사이버 기업의 경우 양자내성암호 알고리즘으로 다시 암호화를 진행할 데이터 자산을 포함하는 인벤토리 구축을 고려를 제시하였다.[11]

이렇듯 세계의 주요 국가와 기관에서는 다가오는 양자 컴퓨터의 위협에 디지털 세계를 보호하기 위해서 암호체계 전환의 중장기적 계획을 세우고 전환을 시작하였다.

〔표 4〕 WEF, 양자 안전 전환의 프레임워크

단계	추진 정책	세부내용
1단계	양자 보안 비전 설정	조직이 양자 기술에서 안전한 생태계로 전환하고 양자 위협을 줄이도록 만듦
2단계	변화의 동인 파악	양자 위협 현실화, 규제적 압박, 시장 역동성, 암호화 관리 수요
3단계	양자 보안 로드맵 수립	인재 및 교육, 관리 및 절차, 기술 및 인프라
4단계	주요 성공 요인 시행	표준과 인증 제도, 생태계 협력, 기술적 혁신과 연구, 지속적이고 장기적인 기업 투자

Ⅲ. 양자내성암호 적용 사례

본 장에서는 국내·외 신업계에서의 양자내성암호를 적용하여 성능을 분석한 사례와 상용화 동향에 대하여 살펴본다.

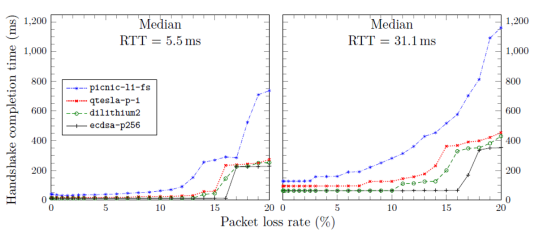
3.1. 양자내성암호 적용 현황

미국은 산업계를 중심으로 NIST가 선정하는 표준 양자내성암호 알고리즘으로 적용하여 성능을 확인하고 있으며 주로 기업을 중심으로 양자내성암호를 적용하고 있다. 국내에서도 국제망에 양자내성암호를 적용하는 등 국제적으로 양자시대에 경쟁력을 갖추고자 노력하고 있다.

3.1.1. 국외 양자내성암호 적용 사례

마이크로소프트와 워털루 대학 연구진은 '20년 하이브리드 키 교환 알고리즘 네트워크 적용 테스트를 수행했다.[12] Frodo, SIKE, Kyber 알고리즘을 적용하여 키 교환 메커니즘의 핸드셰이크 완료 시간을 확인했으며, 고품질 네트워크 링크(패킷손실률 1% 이하)에서 암호화 계산 시간이 주요 영향을 미치는 요인 이었으며, ECDH, Kyber, Frode의 경우 암호화 처리 시간이 약 2ms 미만임에 따라 핸드셰이크 완료 시간이 비슷했다. 반면 패킷손실률이 5% 이상으로 증가하면서 더 큰 공개키와 암호문을 사용하는 키 교환 메커니즘은 더 많은 패킷을 유도함으로써 [그림 1]과 같이 완료시간이 증가되는 것을 확인할 수 있다.

일본의 NICT((National Institute of Information and Communications Technology, 정보통신연구기구)는 '22년 일본 보안 전문기업 Toppan 및 글로벌 기업과 CRYTSTALS-Dilithium 알고리즘이 적용된 스마트카드를 개발했으며 H-LINCOS(의료기관이 디지털 의료기록 데이터를 백업 및 상호이용할 수 있도록 지원하는 시스템)에 스마트 카드 인증, 의료 데이터의 안전한 저장과 교환 등에서 성공적으로 테스트를 완료했다. 또한 25년에는 제한적으로 적용하며 30년에는 PQC 스마트 카드와 관련된 서비스를 시작할 것을 목표로 추진할 것이라 밝혔다.[13]



〔그림 1〕 키 교환 알고리즘 네트워크 테스트

3.1.2. 국내 양자내성암호 적용 사례

SKT와 SKB는 '22년 9월 국제망을 이용하는 글로벌 VPN 네트워크에서 양자내성암호를 상용화했다고 밝혔다. PQC-VPN에 적용한 알고리즘은 NIST가 선정한 양자내성암호 알고리즘 최종 후보인 Kyber와 Dilithium이며 미국, 일본, 싱가폴 등 해외에서 네트워크 테스트를 성공했다.[14]

LG유플러스는 '22년 6월 세계 최초로 격자 기반의 양자내성암호 기술을 탑재한 광전송장비(ROADM)를 개발하고 다양한 산업에서 실증했으며 한국정보통신기술협회(TTA)로부터 성능검증을 완료했다. 10월에는 하이브리드 방식의 양자내성암호와 물리적 복제 방지 기술(PUF)를 적용한 VPN을 개발해 23년도 상반기에 상용화할 예정이다. 또한 CES 2023에서 양자내성암호를 적용한 커넥티드카 보안기술 AVN(오디오, 비디오 내비게이션), 생체인증 기반의 결제 서비스 등을 선보였다.[15]

Ⅳ. 결 론

양자컴퓨터는 빠른 속도로 발전하고 있다. 양자컴퓨터가 빠른 속도로 방대한 데이터를 처리할 수 있는 성능은 기존 암호체계의 위협 요인이다. 본논문에서는 미국을 비롯해 주요 국가들이 이러한 위협 요인에 대응하기 위해 양자내성암호 전환을 어떻게 준비하고 있는지를 살펴보았다. 대부분의 국가에서는 우선적으로 표준화, 로드맵 마련 등의 전략을 수립하고 전환에 필요한 기술력을 갖추는 단계로 진행하고 있다. 또한 산업계에서는 제품에 국가 표준알고리즘을 적용해 성능을 테스트하거나 제품화를 통해 향후 다가오는 양자시대에서 시장 경쟁력을 갖추고자 준비하고 있다.

국내의 경우 KpqC 프로젝트를 통해 국산 양자내성암호 알고리즘을 개발하고 있지만 전환을 위한 계획, 절차 등은 부재한 상황이다. 양자내성암호 전환은 완전히 다른 알고리즘을 대체하는 것으로 기존 시스템에서 교체되어야 할 알고리즘을 찾고, 적합한 알고리즘으로 교체, 테스트를 통해 정상적으로 동작 가능한지를 확인하는 등 많은 노력과 시간이 소요될 것이다. 그렇기 때문에 지금부터라도 중장기 관점에서의 전환 체계를 마련하고 전환을 시작해야 한다.

참 고 문 헌

[1] nature, GOOGLE PUBLISHES LANDMARK QUANTUM SUPREMACY CLAIM, 2019. 9월

[2] Peter W Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Journal on Computing 26.5, pp.1484-1509, 1997

[3] NIST Post-Quantum Cryptography Project, https://csrc.nist.gov/Projects/post-quantum-cryptography, Post-Quantum Cryptography

[4] NIST NCCoE, MIGRATION TO POST-QUANTUM CRYPTOGRAPHY, 2021.8월

[5] DHS, PREPARING FOR POST-QUANTUM CRYPTOGRAPHY, 2021.10월

[6] Executive Order on Enhancing the National Quantum Initiative Advisory Committee (EO 14073), 2022. 5월

[7] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 2022. 5월

[8] ETSI, Quantum-Safe Cryptography (QSC) Quantum-safe algorithmic framework, 2016.7월

[9] ETSI, Migration strategies and recommendations to Quantum Safe schemes, 2020. 8월

[10] ANSSI, “ANSSI views on the Post-Quantum Cryptography transition”, https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/, 2022.1월

[11] WEF, "Transitioning to a Quantum-Secure Economy", 2022.9월

[12] Christian P., Benchmarking Post-Quantum Cryptography in TLS, 2020.

[13] TOPPAN, https://www.toppan.com/en/news/2022/10/newsrelease221024_1.html, 2022.10월

[14] SKT SKB, https://news.sktelecom.com/181250, 2022.9월

[15] LG유플러스, https://www.lg.co.kr/media/release/25469,https://www.lguplus.com/about/ko/corporation/promotion/press-kit/detail/2000000252

〈저 자 소 개〉

유 다 은 (Da Eun Yoo)

2015년 2월 : 숙명여자대학교 컴퓨터과학과 졸업
2017년 9월~현재 : 한국인터넷진흥원 차세대암호기술팀 선임연구원
<관심분야> 정보보호

김 준 섭 (Jun-Sub Kim)

2010년 2월 : 순천향대학교정보보호학과 졸업
2012년 2월 : 순천향대학교정보보호학과 석사
2015년 2월 : 순천향대학교정보보호학과 박사
2015년 3월~2016년 1월 : 성균관대학교IT융합연구원박사후연구원
2016년 2월~2016년 11월 : 한국지역정보개발원책임연구원
2017년 3월~현재 : 한국인터넷진흥원책임연구원
<관심분야> 정보보호, 암호알고리즘

김 기 문 (Ki-moon Kim)

2017년 2월 : 고려대학교 정보보호대학원 석사
2023년 3월 : 고려대학교 정보보호대학원 박사과정
2011년 9월~현재 : 한국인터넷진흥원(KISA) 차세대암호기술팀 팀장
<관심분야> 정보보호, 암호알고리즘, 랜섬웨어, 양자내성암호 등