NIST PQC 표준화 PROJECT 동향

신다윗, 김호원
부산대학교

dawit@islab.re.kr, howonkim@gmail.com

Trends of NIST PQC Standardization Project

Shin Da Wit, Kim Ho Won
Pusan National Univ.

요 약

PQC 표준의 최종 버전 및 PQC 전환 보고서가 공개될 예정이다. PQC 표준의 최종 버전 및 PQC 전환 보고서가 공개되기 전까지, NIST의 PQC 표준화 프로젝트 진행 상황을 살펴보고자 한다. 이에는 PQC 표준화 공모, FIPS 표준 초안, 그리고 PQC 전환의 진행 상황이 포함된다.

Ⅰ. 서 론

공개키 암호화 방식인 RSA와 ECC는 Shor의 알고리즘에 의해 다항 시간 내에 공격당할 수 있으며 대칭키 암호화 알고리즘인 AES는 Grover 알고리즘을 통한 무차별 공격으로 인해 키 전수조사를 O(N)에서 (√ N)으로 할 수 있기 때문에, 보수적으로 접근하였을 때 기존 대비 키 길이를 두 배로 늘려야 같은 수준의 암호 강도를 유지할 수 있다. [1, 2]

RSA 및 AES에 대한 공격은 양자 컴퓨터의 성능이 충분히 발전하여 Shor 및 Grover 알고리즘을 실행할 수 있는 경우에 가능할 수 있다. 양자컴퓨터를 개발하는 기업들로 IBM, 구글, MS 등 많이 있다. 이 기업들 중에서 대표적으로 IBM의 양자 컴퓨터 발전 상황을 보면, 2023년 12월 4일에 고품질 큐비트를 가진 IBM Quantum Heron 133 큐비트를 발표했다. IBM의 양자 개발 및 혁신 로드맵에 따르면, 2033년까지 약 2,000 큐비트와 10^9 게이트를 개발할 예정이다. [3, 4]

표1. 양자 컴퓨터의 RSA 및 ECC 공격 자원 추정치

암호	큐비트	Toffoli gate
256비트 ECC의 ECDLP	2,330	1.26x10^11
1,024비트 RSA	2,050	5.81x10^11
2,048비트 RSA	4,098	5.20x10^12

위 내용을 통해 IBM의 양자 컴퓨터의 개발이 RSA와 ECC를 공격하기 위한 양자 컴퓨터의 자원 추정치에 가까워짐을 알 수 있다[표1]. 이는 RSA 및 ECC의 암호가 무력화될 시점이 가까워지고 있다는 것을 나타낸다. 그러나 양자 컴퓨터의 큐비트의 품질 및 게이트 충실도에 따라 이러한 암호 체계 공격을 위한 양자 컴퓨터의 자원 추정치가 달라질 수 있다. [5]

현재 충분한 성능의 양자 컴퓨터가 없어 Shor 및 Grover 알고리즘이 공개키 및 대칭키 암호를 공격할 수 있는 상황은 아니지만 "Harvest Now, Decrypt Later" 공격에 대비해야 한다. 이는 공격자가 현재 공개 통신 채널을 통해 암호화된 데이터를 수집하고 저장한 후, 데이터 복호화 기술이 좋아지면 저장된 데이터를 복호화하는 전략이다. 따라서 현재 데이터들의 기밀성을 지속적으로 유지하기 위해 현재 데이터의 암호화 체계를 양자내성암호(PQC) 체계로의 전환을 고려해야 한다. [6]

모스카 정리를 활용하면 조직이 양자내성 암호 체계로 전환할 필요성을 파악할 수 있다. 이는 데이터의 보안을 유지해야 하는 시간을 x, 암호화 시스템을 업그레이드하는 데 걸리는 시간을 y, 그리고 현재 암호화를 깨뜨리는 예상 시간을 z로 정의한다. 이때, x+ y>z 및 y>z을 만족한다면 암호 전환을 고려해야 함을 의미한다. [7]

기존의 암호 체계를 새롭게 전환하기 위해 클래식 컴퓨터뿐만 아니라 양자컴퓨터를 이용한 공격이 다항 시간내에 불가능한 양자내성암호를 설계해야 한다.

Ⅱ. 본론

NIST는 2016년 12월 20일에 PQC 표준화 공모전을 시작하여 2022년 7월 5일에 공개키 암호화 및 키교환(PKE/KEM)과 전자서명(DSA) 알고리즘 표준을 선정했다[표2]. 이어서 표준을 선정한 후에는 공개키 암호화/키교환에 대한 4차 라운드 평가가 현재까지 진행 중이다.

표2. 3차 Round에서 선정된 PQC 표준 알고리즘

알고리즘	기반 문제	기능	표준 초안
CRYSTAL-KYBER	격자기반 (Lattice)	공개키암호화(PKE) 키암호화(KEM)	FIPS 203
CRYSTAL-DILITHIUM	격자기반 (Lattice)	전자서명(DSA)	FIPS 204
FALCON	격자기반 (Lattice)	전자서명(DSA)	FIPS 204
SPHINCS+	Stateless Hash기반	전자서명(DSA)	FIPS 205

4차 라운드에는 BIKE, Classic McEliece, HQC 알고리즘이 있다. SIKE는 자신들이 설계한 아이소지니 기반 암호가 Castryck 및 Decru 계열 공격에 안전하지 않다는 것을 인정하였기 때문에 3개의 후보만 남게 되었다. 이들 후보에 대한 평가는 18~24개월 동안 진행될 예정이므로, 올해 7월 안에 최종 표준이 발표될 것으로 예상된다. [8]

전자서명 알고리즘 1차 라운드는 격자 기반이 아닌 전자서명 알고리즘을 선정하기 위한 목적으로

진행중이다. 1차 라운드를 통해 50개의 후보 알고리즘 중 40개가 선정되었고 몇 달 후에 2차 라운드를 위한 전자서명 알고리즘 선발이 있을 예정이다. [9]

PQC 표준으로 선정된 알고리즘들을 구현할 때는 미국 연방 정보 처리 표준(FIPS) 초안을 참고하면 된다. 다만, 이 초안은 알고리즘 구현을 위한 일반 요구사항을 지정하는 것일 뿐, 특정 구현의 안전성을 보장하지는 않는다. 모든 모듈이 안전한 방식으로 설계되고 구축됐는지 확인하는 것은 구현자의 책임이다.

FIPS 203 초안은 모듈 격자 기반 오류 학습 키 암호화(ML-KEM) 메커니즘(키 생성, 암호화, 복호화) 및 매개변수 세트(ML-KEM-512, ML-KEM-768, ML-KEM-1024)에 대한 표준을 설명하는 문서이다. NIST에서는 ML-KEM-768을 기본 매개변수 세트로 사용하도록 권장한다. 그리고 KEM의 일반적인 특성에 대해 자세히 논의하기 위해 특별 출판물(SP) 800-227 문서가 나올 예정이다. 여기에는 보안 애플리케이션에서 KEM을 사용하기 위한 기본 정의, 보안 속성 및 요구 사항이 포함된다. [10]

FIPS 203 초안에 대한 현재 계획이 5차 PQC 표준화 회의에서 논의되었다. 이에 따라 다음과 같은 내용이 포함되었다: 키 생성과 암호화 과정에 있는 A행렬의 인덱싱 방식 변경이 필요하며, 이러한 변경이 호환성에 미치는 영향을 최소화해야 한다. 또한, SHAKE를 위한 XOF API를 명시하여 SHAKE의 표준을 준수할 필요가 있다. 이에 따라 SampleNTT 함수를 다시 작성해야 한다. 또한, 하위 수준의 무작위화 되지 않은 API를 명시하고, 이를 통해 무작위 값을 사용하는 하위 수준의 API에 대한 KATs(Known Answer Tests)를 정의하여 암호화 알고리즘 검증 프로그램(CAVP)을 사용한 테스트를 원활하게 진행할 계획이다. [11]

FIPS 204 초안은 데이터에 대한 무단 수정을 탐지하고 서명자의 신원을 인증하는 모듈 격자 기반 전자서명(ML-DSA)의 매커니즘(키 생성, 전자서명 생성 및 검증)에 대한 표준을 설명하는 문서이다. [12]

FIPS 204 초안에 대한 현재 계획이 5차 PQC 표준화 회의에서 논의되었다. 이에 따라 서명 및 개인 키의 길이 불일치, SHAKE를 사용한 불확실한 출력 길이, 바이트 문자열 처리하는 해시 함수, 검증 과정의 불필요한 힌트 확인 제거, 명시적인 while 루프 반복 제한 등이 주요 내용으로 논의되었다. 뿐만 아니라 FIPS 203과 같은 내용인 CAVP를 사용한 테스트를 위해 하위 수준의 API에 대한 명시적인 정의하는 내용도 다뤄졌다.

FIPS 205 초안은 상태가 없는 해시 기반 전자서명 알고리즘(SLH-DSA)에 대한 표준을 설명하는 문서이다. 이 해시 알고리즘의 가장 큰 단점은 매개변수가 12개라는 것이다. 이에 대한 매개변수 개수 변경에 대한 합의가 이루어지지 않아, 이를 보류했다. 서명의 크기를 줄여 서명 생성 속도를 높이는 의견에 대한 별도의 게시물을 만들어 이 문제를 다룰 예정이다. [13]

NIST의 PQC 표준화 프로젝트는 아직 진행중에 있음을 알 수 있다. 이제 PQC 전환 프로젝트의 진행상황을 알아본다.

양자내성암호화 전환을 진행할 때 살펴봐야할 부분은 5가지가 있다. 각각은 양자 취약 암호화 코드 교체 또는 해당 코드 종속성 제거를 위한 우선순위 측면을 다룬다. 1) FIPS-140 인증 모듈의 양자 취약 공개키 암호화 2) 양자 취약 공개키 암호화 포함 암호화 라이브러리 3) 양자 취약 공개키 암호화 중점 암호화 애플리케이션 4) 컴퓨팅 플랫폼 내장 양자 취약 암호화 코드 5) 양자 취약 암호화 알고리즘 기반 통신 프로토콜이다. [14]

양자에 취약한 부분을 효율적으로 찾기 위해 현재 NIST의 PQC 전환 프로젝트에서는 네트워크 인프라, 통신 하드웨어, 운영체제, 애플리케이션, 통신 프로토콜, 키 인프라, 접근 제어 메커니즘 등에서 공개키 알고리즘 사용 사례를 자동으로 식별할 수 있는 검색 도구를 개발하고 있다. 이 프로젝트에 기술 벤더들이 협력하여 예제 솔루션을 구축 중이며, 예상하는 이슈의 사례들은 NIST SP 1800-38B와 1800-38C 초안에서 확인할 수 있다. [15, 16]

SP 1800-38B는 공개키 애플리케이션 검색 도구의 접근 방식, 아키텍처 및 보안 특성에 관한 초안으로, 여기에는 TLS, SSH 프로토콜, 윈도우 기반 OS 관련 실행/비실행 파일, 리눅스 기반 OS 관련 실행/비실행 파일, 네트워크 트래픽, 키 저장소(ICSF, RACF) 등과 관련된 양자내성 취약점 사례(Use Case)를 확인할 수 있다.

SP 1800-38C는 양자내성암호화 기술의 상호운용성 및 성능 보고서 초안으로, SSH, TLS, QUIC, X.509, 하드웨어보안모듈(HSM) 등에 대한 상호운용성 및 성능 테스트 결과를 담고 있다.

위의 SP 1800 출간물 외에도 NIST의 양자 내성 암호화 전환 프로젝트에 참여한 협력사들이 PQC 전환에 대한 권장 사항을 담은 책을 제작할 예정이다. 이 책은 PQC 전환에 관심 있는 기업 및 조직들에게 유용한 참고 자료가 될 것이다. [17]

Ⅲ. 결론

양자 컴퓨터 기술이 빠르게 발전하고 있어, 암호화 알고리즘을 공격할 수 있는 능력을 갖춘 양자 컴퓨터 등장이 멀지 않았다. 따라서 양자 전환에 대비하여, 사전에 양자에 취약한 암호화가 적용된 영역과 향후 적용이 필요한 영역을 식별하고, 암호화가 사용되는 방식과 모스카 정리를 통해 우선순위를 파악해야 한다. 왜냐하면 운영 시스템 내 하드웨어, 네트워크, 애플리케이션, 클라우드, 서버 등에 광범위하게 사용된 암호화의 종속성을 충분히 인식하지 못한 상태이기 때문이다. 2024년 봄에 NIST의 SP800-227에서 "Migration to Post-Quantum Cryptography Hybrid mode" 보고서가 PQC 전환 과정을 포함하여 발표될 예정이다. 그리고 이어서 여름에는 최종 PQC 표준이 공개될 것이다. 따라서 향후 나오는 이 자료들을 토대로 본격적인 hybrid 체계를 구축을 시작하는 것이 좋다고 생각한다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2024-2020-0-01797)

참 고 문 헌

[1] Shor, P. W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM review, 41(2), pp. 303-332, 1999

[2] Grover, L. K., "A fast quantum mechanical algorithm for database search. In Proceedings of

the twenty-eighth annual ACM symposium on Theory of computing", pp. 212-219, July. 1996

[3] Erin A, Hugh C, “IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, (https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility)

[4] IBM, (https://www.ibm.com/quantum/assets/IBM_Quantum_Development_&_Innovation_Roadmap.pdf)

[5] Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. “In Advances in Cryptology-ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security”, Part II 23 (pp. 241-270), December. 2017

[6] Wikipedia, (https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later)

[7] Mosca, M., "Cybersecurity in an era with quantum computers: Will we be ready?", IEEE Security & Privacy, 16(5), pp. 38-41, 2018

[8] SIKE, (https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf)

[9] Dustin M, (https://csrc.nist.gov/csrc/media/Presentations/2024/update-on-the-nist-pqc-standardization-project/images-media/moody-are-we-there-yet-pqc-pqc2024.pdf)

[10] NIST, (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf)

[11] NIST, (https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program)

[12] NIST, (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf)

[13] NIST, (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.ipd.pdf)

[14] Barker, W., Souppaya, M., Newhouse, W., Dakota Consulting, NIST, August, 2021, (https://www.nccoe.nist.gov/sites/default/files/2022-07/pqc-migration-project-description-final.pdf)

[15] NIST, (https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms)

[16] NIST, “Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards”, December, 2023, (https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1))

[17] AVID, TNO, CWI, “PQC Migration handbook”, December, 2023 (https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf)