KCMVP 인증 상의 PQC 알고리즘 도입 고려사항

박지민[1], 이석준[2]
[1]가천대학교 컴퓨터공학부(스마트보안전공) 학부생
[2]가천대학교 컴퓨터공학부(스마트보안전공) 교수
jimin030907@gachon.ac.kr, junny@gachon.ac.kr

Consideration for Including PQC Algorithms in KCMVP Certification

Jimin Park[1], Sokjoon Lee[2]
[1, 2]Dept. of Smart Security, Gachon University

요 약

양자 컴퓨터가 발전함에 따라 RSA, ECC 등 기존 공개키 암호 알고리즘의 해독 가능성이 점점 커지고 있으며, 이러한 양자 위협에 대응하기 위해 양자 내성을 갖는 암호, 즉 PQC에 관한 연구가 활발하게 이루어지고 있다. 국가·공공기관에서 도입하는 보안 제품에서 암호 기능을 사용시 검증필 암호 모듈 탑재가 필요하지만, 현재 NIST는 표준화 대상 알고리즘만 선정하였을 뿐 국내외 모두 표준화가 완료되지 않아 PQC는 KCMVP 검증대상 암호로 포함되어 있지 않다. 본 논문에서는 KCMVP(국내 암호모듈 검증 체계)와 PQC의 최근 동향을 알아보고 KCMVP에 PQC알고리즘을 도입할 때의 고려 사항에 대해 분석한다.

1. 서론

국내에서는 국가·공공기관에서 활용하는 암호모듈의 안전성을 평가하기 위하여 한국형 암호모듈 검증 프로그램(Korea Cryptographic Module Validation Program, KCMVP)을 도입한 바 있다. 하지만 최근 양자 컴퓨터의 등장으로 인해 RSA, ECC와 같은 기존 공개키 암호 알고리즘이 무력화될 것으로 예상하여 양자컴퓨터를 활용한 공격 시도로부터 안전한 양자내성암호(Post Quantum Cryptography, PQC) 관련 연구가 활발하게 이루어지고 있다.

현재 KCMVP 인증 제도에 PQC 알고리즘은 포함되어 있지 않으며, 차후 NIST 혹은 KPQC 표준 알고리즘 선정 및 표준화 완료 후 포함될 것으로 보인다. PQC 알고리즘이 KCMVP 인증 제도에 포함되기 위한 검증 과정에는 시험 방법, 시험을 위한 벡터값 등 고려해야 할 요소들이 있을 것이다. 따라서 본 논문에서는 먼저 KCMVP 및 PQC 표준화 동향을 살펴보고, KCMVP 인증 대상 알고리즘에 PQC가 포함될 때의 고려사항을 제안한다.

2. KCMVP 동향

미국과 캐나다가 공동으로 암호모듈 검증을 시행하기 위해 1995년 CMVP를 시작하였고, 이후 국내에서도 2010년부터 KCMVP를 운영하기 시작했다. KCMVP는 국가정보통신망에서 소통·저장되는 비밀이 아닌 업무자료를 보호하기 위해 국가·공공기관에서 도입하는 암호모듈의 안전성과 구현 적합성을 검증하는 제도[1]이다. 현재 260개의 검증필 암호모듈이 KCMVP 목록에 등재되어 있다. 현재 유효한 검증필 암호모듈은 92개이며, 나머지는 만료되거나 포기한 것으로 보인다. 모듈의 형태는 소프트웨어, 펌웨어, 하드웨어 그리고 이 세 가지 형태를 조합한 형태로 구현 가능하다.

국가·공공기관이 도입하는 보안 기능이 탑재된 IT제품은 보안적합성 검증을 시행하며, KCMVP 검증필 암호모듈이 일부 제품의 도입 요건으로 활용된다. 가상사설망(VPN), 소프트웨어 기반 보안USB제품, 호스트 자료유출방지제품, 통합인증제품(SSO), 문서암호화제품(DRM), DB암호화제품, 구간암호화제품 등은 도입을 위해 검증필 암호모듈을 필수적으로 탑재해야 한다[2]. 예를 들어 공공·국방과 같은 분야에서 활용하는 드론의 경우, 보안을 위하여 통신구간 암호화가 필요할 것이며 이 경우 KCMVP 검증필 암호 모듈을 탑재해야 도입이 가능할 것으로 보인다.

3. PQC 표준화 동향

2017년부터 NIST에서는 Post Quantum Cryptgraphy(PQC) 알고리즘 표준화를 진행 중이다.

2022년 표준화 대상 알고리즘으로 CRYSTALS-Kyber 등 4종의 PQC 알고리즘을 선정[3]했으며 현재 1라운드 추가 전자서명 공모를 진행 중이다. 2023년 8월, PQC 알고리즘 표준화 문서 초안으로 Module-Lattice-Based Key-Encapsulation Mechanism Standard[4]와 Module-Lattice-Based Digital Signature Standard[5]를 의견수렴을 위해 공개하였으며, 특히 CMVP에 PQC를 포함할 것을 언급한 바 있다[6].

4. KCMVP 인증 제도 포함 시 고려사항

4.1 KCMVP 인증 시험 기본 검증 사항

구분	고려사항
기본 검증사항	- 파라미터 값 설정 - 변수 범위 - 함수 입출력 값
	- PQC 내부 알고리즘 추가
양자안전성	- 양자안전성 검증

KCMVP 인증을 위해서는 해당 알고리즘 내 각각의 단계 입·출력값이 정상적으로 입력되고 전달되는지 확인하는 것뿐만 아니라 알고리즘 내 함수에 대한 검증도 함께 포함되어야 할 것이다.

이를 위해, NIST의 PQC 표준 알고리즘 중 CRYSTALS-Kyber, CRYSTALS-Dilithium을 기준으로 고려사항을 정리하고자 한다. 현재 검증대상 알고리즘에서 해시함수는 SHA-2 (SHA-224, SHA-256)가 대부분 사용되고 있으며, SHA-3 또한 검증대상 알고리즘에 포함되어 있고, 이 중 고정길이 출력을 생성하는 SHA3-224, SHA3-256 등이 여기에 해당된다. CRYSTALS-Kyber와 CRYSTALS-Dilithium에서는 SHA-3 중 임의 크기 출력을 생성하는 SHAKE-128, SHAKE-256 등이 사용되고 있으나, 이들은 KCMVP에 해당되지 않으므로[7] 검증대상 알고리즘으로 포함되어야 할 것이다.

4.2 PQC 알고리즘의 양자안전성 검증

PQC 알고리즘을 KCMVP 인증 제도에 포함하기 위한 이유는 추후 양자컴퓨터 환경에서도 안전한 모듈을 제작하기 위함이므로, PQC 알고리즘 역시 KCMVP 알고리즘에 포함되더라도 양자컴퓨터 환경에서도 안전한지를 지속적으로 검증하여야 할 것이다.

ETRI(한국전자통신연구원)를 중심으로 암호에 대한 양자안전성 연구[8]가 이루어지고 있다. 해당 연구는 양자컴퓨터 기반 암호 해독에 필요한 소요시간 등을 계산하여 PQC 등의 양자안전성을 검증하는 것이 목적이다. 이와 같은 연구를 통하여 양자안전성 검증 기술이 도입된다면, 쇼어 알고리즘 등 양자 공격으로부터 더욱 안전한 암호체계를 갖출 수 있을 것이다.

5. 결론

본 논문에서는 KCMVP의 동향과 함께 최근 양자컴퓨터의 등장으로 인해 대두되고 있는 PQC의 표준화 동향을 소개했다. 나아가 PQC가 KCMVP 검증대상 알고리즘에 포함될 때의 고려사항을 제안했다. 최근 NIST에서 CMVP에 PQC를 포함하겠다는 내용을 언급함에 따라 국내에서도 KCMVP에 PQC를 포함하는 것을 고려할 시기이다. 이를 위해 PQC 알고리즘에 맞는 암호모듈 검사 체계 구축이 필요하며 PQC의 양자안전성을 검증할 수 있도록 활발한 관련 연구가 필요할 것임을 언급하였다.

본 논문은 NIST에서 표준으로 지정한 CRYSTALS-Kyber와 CRYSTALS-Dilithium을 중심으로 작성하였으나, 차후 KPQC 공모를 통해 선정되는 암호에 대해서도 KCMVP 인증 제도에 포함하기 위한 고려사항에 대해서도 연구하고자 한다.

6. Acknoledgment

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2023-00225201, 국방 무인이동체 역이용 방지 제어권 보호기술 개발)

참고문헌

[1] 국가정보원, 국가보안기술연구소 “검증필 암호모듈 운용가이드”, 2022

[2] 국가사이버안보센터 “보안적합성검증”, https://www.ncsc.go.kr:4018/PageLink.do

[3] NIST, “Post-Quantum Cryptography Selected Algorithms 2022”, https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[4] NIST, “FIPS 203 (draft), Module-Lattice-Based Key-Encapsulation Mechanism Standard”, 2023

[5] NIST, “FIPS 204 (draft), Module-Lattice-Based Digital Signature Standard”, 2023

[6] NIST, “FIPS 203 (Initial Public Draft) Module-Lattice-Based Key-Encapsulation Mechanism Standard”, 2023

[7] 암호모듈 시험기관, “SHA-3 검증시스템”, 2019

[8] 최두호, 강유성, 이석준, “〈Q|Crypton〉 : 암호 양자안전성 검증 기술”, 정보보호학회지, 33(1), 7-12, 2023