정적·동적 분석을 통한 양자취약암호(Non-PQC) 탐지도구 개발에 관한 연구

정진호*, 서정민*, 신찬희*, 하준수*, 문재현*, 윤기순*

*중부대(대학생), *중앙대(대학생), *이화여자대(대학생), *한국항공대(대학생),
*한국기술거래사회(교신저자), *NSHC(교신저자)

Research on Static and Dynamic Detection Systems for Non-PQC Vulnerabilities

Jinho Jung*, Jungmin Seo*, Chanhee Shin*, Junsu Ha*,
Moonjae Hyun*, Kisoon Yoon*

*Joongbu Univ.(Undergraduate), *Chungang Univ.(Undergraduate),
*Ewha Womans Univ.(Undergraduate), *Korea Aerospace Univ.(Undergraduate),
*Korea Technology Transfer Agents Association(Corresponding author),
*NSHC(Corresponding author)

요 약

양자컴퓨팅 기술의 발전으로 인해 기존 암호 알고리즘의 체계가 무력화될 수 있는 위협이 존재한다. 양자컴퓨터 시대로의 전환에 대비하여 본 논문은 이러한 양자취약암호를 탐지하기 위해 시그니처 기반의 정적 분석과 API 후킹 기반의 동적 분석을 결합한 시스템을 제안한다. 시스템 내 사용되는 암호 알고리즘의 취약점을 사전에 탐지하여, 안전한 양자내성암호(PQC)로의 전환에 도움을 제공하고자 한다. 이를 통해 보안 문제에 이바지할 수 있다고 기대한다.

I. 서론

최근 양자컴퓨팅 기술의 급속한 발전으로 인해 현재 사이버 보안을 위해 널리 사용되고 있는 대부분의 공개키 암호 체계가 무력화 될 수 있는 문제점이 대두되고 있다[3]. 예를 들어 인터넷 뱅킹과 블록체인 등에 사용되고 있는 RSA와 타원곡선암호 등이 양자 알고리즘인 쇼어 알고리즘(Shor Algorithm)에 의해 다항 시간 안에 풀리고, 대칭키 암호화 알고리즘이나 해시함수들은 그로버 알고리즘(Grover Algorithm)에 의해 안전성이 절반으로 떨어지게 된다[1][2]. 이러한 잠재적인 보안 위협에 대비하여 미국의 NIST, 프랑스의 ANSSI, 한국의 NSR 등 세계 각국의 보안 및 표준화 관련 기관들을 중심으로 양자내성암호(Post-Quantum Cryptography)를 개발하고 표준화하여 보급하려는 시도가 활발히 진행 중이다. 특히 공공, 국방, 대기업과 같이 대규모 시스템을 운영하는 조직들은 모든 시스템에 내재된 양자취약암호들을 찾아내어 PQC로 전환하는 작업을 수행해야 하는데, 현재 그러한 조직들의 시스템 규모와 형태, 그리고 일반적인 운영자와 개발자들의 소양으로 미루어 볼 때 전환 작업이 전적으로 수동으로 이루어지기보다 자동화된 도구의 도움을 통해 수행되는 것이 권고되고 있다[7].

본 논문에서는 이러한 전환 프로젝트를 수행할 수 있도록 시스템에 존재하는 양자취약암호를 자동탐지하는 기본적인 방법론을 제안하여 이러한 문제를 해결하는데 기여하고자 한다. 특히 가장 기본적인 파일들을 대상으로 한 정적 분석과 동적 분석 방법을 결합하여 시스템에서 양자취약암호를 탐지하는 도구를 개발하는 방법론을 제안한다.

II. 관련 연구

2.1 정적 분석

본 연구에서 제안하는 정적 분석은 실행파일, 소스코드, 인증서/키 파일 등을 직접 실행하

지 않고, 그 내부에 존재하는 고유한 패턴을 식별하여 양자취약암호를 탐지하는 기법이다. 이 방식은 국제 암호 표준에 명시된 특정 값들을 시그니처로 활용하여, 분석 대상에 어떤 암호 알고리즘이 사용되었는지를 식별한다.

정적 분석을 위한 시그니처로는 표준 문서에 정의된 상수 파라미터와 알고리즘 고유 식별자(OID), 함수명을 탐지하기 위한 정규식이 있다.

Table 1. 은 표준 문서를 참고해 일부 발췌한 암호 알고리즘명과 OID 값이다. 이 외에도 PKCS 표준 문서를 통해 공개키 구조와 파라미터에 해당되는 정보를, SEC 표준 문서를 통해 타원곡선암호(ECC)의 파라미터 값들을 알아낼 수 있다[4]. 이처럼 해당 값을 이용하여 정적 탐지 과정에서 이용되는 암호 알고리즘의 여부를 판별할 수 있다[7].

Table 1. Static Detection

Key	Non-PQC	OID
Pubilc Key	RSA	1.2.840.113549.1.1.1
	ECC	1.2.840.10045.2.1
	DSA	1.2.840.10040.4.1
Symmetric Key	AES-128	2.16.840.1.101.3.4.1.2
	3DES	1.2.840.113549.3.7
	RC4	1.2.840.113549.3.4

Table 2. ECC Parameter

Curver	p	a	b	Gx	Gy	n
secp256r1	FFFFFFFF00000001 0000000000000000 00000000FFFFFFFF FFFFFFFF	FFFFFFFF00000001 0000000000000000 00000000FFFFFFFF FFFFFFFC	5AC635D8AA3A93E7B 3EBBD557B6986BC65 1D06B0CC53B0F63BC E3C3E27D2604B	6B17D1F2E12C4247F8 BCE6E563A440F27703 7D81DE2B33A0F4A13 945D898C296	4FE342E2FE1A7F9B8E E7EB4A7C0F9E162CB 0654B1D1ABEBAA4A E8997AC90FB0	FFFFFFFF00000000FF FFFFFFFFFFFFBCE6 FAADA7179E84F3B9C ACFC0632551
brainpoolP256r1	A9FB57DBA1EEA9B CE66823A0B3D3BD 726E3BF823OS262	7D5A0975FC2C305 7EEF875D0117AFFE 7FB8055C126DC5C	26DC5C6CE94A4B4 4F30B5E0989D77C 5F8A41B6296CF7E	8BD2AEB9CB7E57C B2C4B46FFCB1B7 AF8BDE27E13BD2	547EF835C3DAC4F D97F961A1461 1D C9C2774513ZED8	A9FB57DBA1EEA9B CB5B60A0B3BBD 718C397AA3B561A

2.2 동적 분석

시그니처 기반의 정적 분석에서 자체 암호 알고리즘을 사용하거나, 난독화가 되어있으면 양자취약암호 알고리즘을 탐지하기 어렵다.

본 연구에서는 정적 분석의 한계를 개선하기 위해 동적 분석을 함께 수행한다. 실행파일이 동작하는 과정 중, 주요 암호 라이브러리의 API 호출을 가로채는 후킹(Hooking) 기술을 기반으로 동작한다.

사전에 정의한 Wrapper 함수가 실행되어 알고리즘 종류, 키 길이, 초기화 벡터 등의 데이터를 저장한 후 원본 함수를 호출하여 정상적인 동작을 수행한다. 이 과정을 통해 정적 분석으로 확인이 어려운 대칭키 길이를 파악하거나, 별도의 암호화 모듈을 로드하는 과정을 탐지할 수 있다[5].

Table 3. Dynamic Detection

OS	Library
Common	OpenSSL
	GnuTLS
	NSS
Linux	Linux AF_ALG
	cryptodev

III. 제안하는 탐지 시스템

Fig 1. Detection System Flowchart

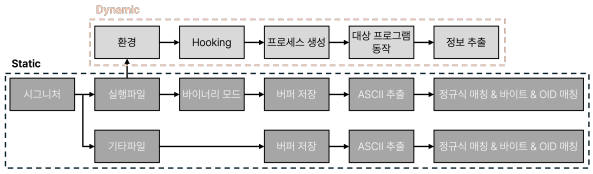


Fig 1.과 같이 본 논문에서 제안하는 탐지 시스템은 분석 대상 파일의 특성에 따라 최적의 분석 방법을 적용하고, 정적·동적 분석 기법의 결과를 종합하여 양자취약암호 탐지율 향상을 목표로 한다.

분석 대상에 해당되는 파일의 유형을 식별한 다음, 해당 파일에 대해 정적 분석 단계가 진행된다. Table 1.과 같이 암호 알고리즘명의 정규식, 고유 파라미터 및 OID 등을 기준으로 양자취약암호을 식별한다. 만약 분석 대상이 실행파일인 경우, 추가적으로 동적 분석 과정을 거친다. Table 3.에 명시된 주요 암호 라이브러리를 대상으로 후킹을 적용해 프로그램 실행 중 호출되는 암호 함수의 종류와 키 길이 등의 정보를 실시간으로 확인한다. 동시에 진행되는 두 과정을 통해 난독화된 코드나 로드되는 라이브러리 내 함수 사용을 방지할 수 있다.

이러한 통합 방식은 빠른 속도로 넓게 탐지하는 정적 분석의 장점과, 동적 분석의 정확성을 결합하여 기존 한계를 보완하고 양자취약암호를 효율적으로 찾아낸다.

IV. 결론

본 논문은 시그니처 기반의 정적 분석과 미탐 개선을 위해 동적 분석을 결합한 양자취약

암호 탐지 시스템을 제안한다.

제안된 시스템은 파일 종류에 따라 분석 방식을 달리 적용한다. 소스코드와 같은 정적 파일은 시그니처 기반의 빠른 정적 분석을 통해 검사하고, 실행 파일에 대해서는 정적 분석의 한계를 보완하기 위해 API 후킹 기반의 동적 분석을 함께 수행하여 분석의 정확도를 높일 수 있는 방안을 제시한다. 이를 통해 시스템에서 사용되는 암호 알고리즘의 취약점을 사전에 식별하고, 안전한 PQC로의 전환에 실질적인 도움을 받을 수 있을 것이라고 예상한다.

앞으로 발생할 양자취약암호의 시그니처 기반 정보를 추가하고, 후킹 방식의 동적 분석에서 라이브러리 이상의 내용을 탐지할 수 있도록 결합하여 양자컴퓨팅 기술로부터 보다 안전한 암호 체계를 마련할 수 있을 것이다.

[Acknowledgement]

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (RS-2024-00399401, 양자안전 보안인프라 전환 및 대양자 복합 안전성 검증기술 개발)

[참고문헌]

[1] Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20-22 November 1994.

[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, Philadelphia PA, USA, 22-24 May 1996.

[3] Zhang M, Wang J, Lai J, Dong M, Zhu Z, Ma R, Yang J. Research on Development Progress and Test Evaluation of Post-Quantum Cryptography. Entropy. 2025, 27, 212.

[4] Pasupuleti, Murali Krishna. (2025). Post-Quantum Cryptography: Algorithms and Implementation Challenges. International Journal of Academic and Industrial Research Innovations(IJAIRI). 05. 234-243. 10.62311/nesx/rphcrcscrbc4.

[5] Dang, Q. H. (2025). A Survey of Post-Quantum Cryptography Support in Cryptographic Libraries. arXiv preprint arXiv:2508.16078.

[6] O-RAN Alliance. (2023). Research Report on Quantum Security. O-RAN Alliance.

[7] National Institute of Standards and Technology. "Cryptographic Algorithm Object Registration." Computer Security Resource Center, csrc.nist.gov/projects/computer-security-objects-register/algorithm-registration. Accessed 13 Oct. 2025.