https://doi.org/10.33778/kcsa.2024.24.2.071

NIST PQC 표준화 과정 및 Round 4 선정/비선정 알고리즘 분석★

최 유 란*, 최 윤 성**, 이 학 준*

요 약

양자 컴퓨팅의 급속한 발전으로 현재의 공개키 암호화 방식이 취약해지자, 미국의 국립표준기술연구소(NIST)는 양자 컴퓨터 공격에 대응할 수 있는 새로운 암호화 표준을 개발하기 위한 Post-Quantum Cryptography(PQC) 프로젝트를 시작했다. 이 프로젝트는 전 세계 연구자들이 제안한 다양한 암호 알고리즘들을 검토하고 평가하는 과정을 포함한다. 초기에 선택된 양자 저항성 암호화 알고리즘은 격자와 해시 함수를 기반으로 개발됐다. 현재는 BIKE, Classic McEliece, HQC 등 다양한 기술적 접근 방식을 제공하는 알고리즘들이 네 번째 라운드에 검토 중이다. CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON, SPHINCS+는 세 번째 라운드에서 표준화 대상으로 선정됐다. 2024년에는 네 번째 라운드에서 선정된 알고리즘들과 현재 평가 중인 알고리즘들에 대한 최종 결정이 내려질 예정이다. 양자 컴퓨팅 시대를 대비해 공개 키 암호 시스템의 보안을 강화하는 중요한 단계로, 미래의 디지털 통신 시스템을 위협으로부터 보호하는 데 큰 영향을 미칠 것으로 예상된다. 본 논문에서는 양자 내성 암호 알고리즘의 보안성과 효율성을 분석하여 그 동향을 제시한다.

Analysis of NIST PQC Standardization Process and Round 4 Selected/Non-selected Algorithms

Choi Yu Ran*, Choi Youn Sung**, Lee Hak Jun*

ABSTRACT

As the rapid development of quantum computing compromises current public key encryption methods, the National Institute of Standards and Technology (NIST) in the United States has initiated the Post-Quantum Cryptography (PQC) project to develop new encryption standards that can withstand quantum computer attacks. This project involves reviewing and evaluating various cryptographic algorithms proposed by researchers worldwide. The initially selected quantum-resistant cryptographic algorithms were developed based on lattices and hash functions. Currently, algorithms offering diverse technical approaches, such as BIKE, Classic McEliece, and HQC, are under review in the fourth round. CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON, and SPHINCS+ were selected for standardization in the third round. In 2024, a final decision will be made regarding the algorithms selected in the fourth round and those currently under evaluation. Strengthening the security of public key cryptosystems in preparation for the quantum computing era is a crucial step expected to have a significant impact on protecting future digital communication systems from threats. This paper analyzes the security and efficiency of quantum-resistant cryptographic algorithms, presenting trends in this field.

Key words : NIST, QPC Algorithm, Public-Key Encryption, Quantum Computer

접수일(2024년 04월 05일), 게재확정일(2024년 05월 27일)

★ 본 과제(결과물)는 2022년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다.(2021RIS-003)

* 경남대학교/컴퓨터공학부(주저자, 교신저자)
** 인제대학교/AI소프트웨어학부(공동저자)

1. 서 론

양자 컴퓨팅 기술의 급속한 발전은 기존 암호 체계에 중대한 위협을 가하고 있다. 양자 컴퓨터의 이론적 능력은 현재 널리 사용되는 공개키 암호화 방식인 RSA 및 ECC(타원곡선 암호)와 같은 알고리즘을 쉽게 해독할 수 있는 수준에 도달했다. 이는 디지털 통신의 보안을 핵심으로 하는 현대 사회에 있어 중요한 문제를 야기할 수 있다. 양자 컴퓨팅의 발전은 이러한 암호 체계의 취약점을 노출시키며, 금융 거래, 개인 정보 보호, 국가 안보 등 다양한 분야에서 활용되는 암호화 기술에 대한 근본적인 재평가를 요구하고 있다.

이러한 문제를 해결하기 위해 미국 국립 표준 기술 연구소(NIST)는 Post-Quantum Cryptography(PQC) 프로젝트를 시작했다. 이 프로젝트의 목표는 양자 컴퓨터로부터 안전한 새로운 암호화 표준을 개발하는 것이다. NIST는 2016년에 전 세계 연구자들로부터 PQC 알고리즘을 공모하였으며, 이후 여러 단계의 검토와 평가를 통해 알고리즘을 선별했다. 제안된 알고리즘은 수십 개에 달하며, 이들은 보안성, 효율성, 실용성 그리고 기존 시스템과의 호환성 등 다양한 기준에 따라 평가됐다. 평가 과정은 매우 철저하게 진행됐는데, 초기 단계에서는 기술적 검토와 공개 평가를 통해 알고리즘의 보안 수준과 실용적 적용 가능성을 평가했다. 이 과정에서 공개키 암호, 디지털 서명, 키 교환 메커니즘 등 다양한 분야에서 제출된 알고리즘들이 다방면에서 검토됐다. NIST는 이러한 평가 과정을 통해 알고리즘들을 여러 라운드에 걸쳐 선별하고, 각 단계마다 전문가 커뮤니티의 평가와 피드백을 반영하여 최종적으로 양자 컴퓨터에 견딜 수 있는 표준 암호 알고리즘들을 선정했다.

표준화 과정의 마지막 단계에서는 선정된 알고리즘들에 대한 공개적인 피드백을 받고 최종 검토를 진행한 후 공식적인 NIST PQC 표준으로 발표된다. 이 과정은 전 세계적으로 투명하게 진행됐으며, 최종 표준은 국제적으로 인정받고 널리 사용될 것으로 기대된다. 본 프로젝트는 지속 가능한 기술 표준을 마련함으로써 디지털 세계의 보안 강화에 기여할 것으로 보인다. NIST PQC 후보 알고리즘은 (그림 1)과 같이 표준화된 CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON, SPHINCS+ 알고리즘들이 있고, Round 4에서 Classic McEliece, HQC, SIKE 알고리즘들이 선별됐다.

본 논문에서는 NIST가 진행 중인 PQC 표준화 과정(현황)[1] 및 그 과정에서 선정 또는 비선정된 알고리즘들에 대한 동향을 알아보고자 한다. 2장에서는 표준화 대상 알고리즘에 대한 동향을, 3장에서는 Round 4에 선정된 알고리즘들과 비선정된 알고리즘들에 대한 동향을 살펴본다. 4장에서는 본 논문의 결론을 맺는다.

(그림 1) NIST PQC 후보

2. 표준화 대상 알고리즘

PQC 프로젝트의 세 번째 라운드에서는 네 가지 주목할 만한 알고리즘이 선정되어 암호학 분야에서 중요한 발전을 이루었다. <표 1>은 각 알고리즘의 주요 특성을 요약한 표이다. 특히, CRYSTALS-KYBER는 고성능 알고리즘으로, 양자 컴퓨팅의 잠재적 위협으로부터 디지털 통신을 효율적이고 안전하게 보호하는 데 탁월한 성능을 보여준다. 이와 함께, CRYSTALS-DILITHIUM, FALCON, SPHINCS+와 같은 다른 세 알고리즘은 디지털 서명 분야에서 새로운 접근 방식을 제공하며, 각각 보안성, 성능 그리고 다양한 암호학적 응용에서의 적응성 측면에서 특별한 강점을 보여준다. 이러한 알고리즘의 선정은 양자 컴퓨터의 발전에 대비한 안전한 암호화 표준을 마련하는 데 있어 큰 진전을 의미한다.

<표 1> 표준화 후보 알고리즘 특징

알고리즘	스킴	특징
KYBER	격자	키 교환 및 암호화
DILITHIUM	코드	Fiat-Shamir 패러다임 기반의 디지털 서명 알고리즘
FALCON	코드	경량 디지털 서명
SPHINCS+	해시	해시 기반 디지털 서명

2.1 CRYSTALS-KYBER

KYBER는 MLWE(Module Learning With Errors) 문제에 기반한 키 캡슐화 메커니즘(Key Encryption Mechanism, KEM)으로, Unstructured-LWE(Learning With Erros) 문제에 기반한 다른 KEM 디자인에 비해 Structured 접근 방식으로 향상된 효율성을 제공한다. KYBER는 먼저 IND-CPA(Indistinguishability under Chosen Plaintext Attack) 보안을 제공하는 공개키 암호화 스킴(Public-key Encryption, PKE)으로 설계됐으며, 이후 IND-CCA(Indistinguishability under Chosen Ciphertext Attack) 보안을 갖춘 KEM으로 확장했다. 이는 암호화된 메시지가 선택된 평문에 대해 구별이 불가능함을 의미하는 IND-CPA 보안과, 추가적으로 암호화된 메시지가 선택된 암호문에 대해서도 구별 불가능해야 함을 의미하는 더 강력한 IND-CCA 보안을 모두 만족한다.

KYBER는 PQC 시스템으로 개발됐으며, 양자 컴퓨터에 의한 공격으로부터 안전한 것으로 평가되고 있다. 이는 기존의 RSA나 ECC(Elliptic Curve Cryptography) 같은 알고리즘들이 양자 컴퓨터의 발전으로 취약해질 가능성에 대비하기 위한 것이다. KYBER 시스템은 효율적인 키 생성, 암호화, 복호화 과정을 제공하며, 특히 대규모 네트워크에서의 활용을 염두에 두고 설계됐다. 이러한 특성은 KYBER를 클라우드 컴퓨팅, 인터넷 통신, 데이터 보안 등 다양한 분야에서 응용할 수 있도록 한다.

2.2 CRYSTALS-Dilithium

Dilithium은 Module-LWE 가정을 기반으로 한 PQC 디지털 서명 알고리즘으로, 공개 키가 개인 키에 대한 정보를 누설하지 않음으로써 상당한 보안성을 제공한다. 이 알고리즘은 QROM(Quantum Random Oracle Model)에서 강력한 위조 불가능성(Strong Unforgeability under Chosen Message Attack, SUF-CMA)을 보장하며, 특정 서명이 유일한 공개 키가 메시지와 연결될 수 있도록 하는 강력한 결합 속성을 만족시킨다.

성능 최적화를 위해 의사 난수성과 데이터 축소 기술이 사용되며, 숫자 이론 변환(NTT)을 기반으로 한 구현을 통해 효율적인 다항식 곱셈이 가능하다. Dilithium은 Round 3에서 FALCON과 함께 가장 효율적인 서명 프로토콜 중 하나로 평가되었으며, 부동 소수점 산술을 요구하지 않는 장점이 있다.

Dilithium은 강력한 이론적 보안 기반과 뛰어난 성능 특성을 갖춘 Post-Quantum 서명 알고리즘이다. 현재 NIST에서 표준화를 위해 선택된 주요 서명 알고리즘 중 하나이며, 실제 응용 분야에서도 안전하고 효율적으로 사용될 수 있다.

2.3 FALCON

FALCON은 NTRU 격자에서 SIS(Short Integer Solution) 문제에 기반한 안정성을 고려하여 설계된 격자 기반 전자 서명 알고리즘이다. SIS 문제는 양자 알고리즘으로도 효율적으로 해결되지 않는 문제로 알려져 있다. FALCON은 NIST의 Round 3에서 제안된 디지털 서명 스킴 중에서 가장 작은 대역폭(공개 키 크기와 서명 크기의 합)을 가지고 있다.

이 알고리즘은 대역폭이 낮고 검증 속도가 빠른 특징을 가지고 있어 제한된 프로토콜 시나리오에서 우수한 선택으로 간주될 수 있다[2]. 이는 대역폭이 작을수록 암호화된 데이터의 크기가 작아지고, 검증 속도가 빠를수록 서명 검증에 소요되는 시간이 줄어들기 때문이다.

NIST는 FALCON이 올바르게 구현된다는 가정 하에 그 보안성에 확신을 가지고 있으며, 특정 응용 분야에서 작은 대역폭이 필요한 경우를 고려하여 표준화로 선택했다. 이는 FALCON이 효율적이고 안전한 서명 알고리즘으로서의 잠재력을 인정받고 있다는 것을 의미한다.

2.4 SPHINCS+

SPHINCS+는 주어진 해시 알고리즘을 기반으로 한 서명 스킴이다. 이 스킴은 프레임워크이며 SHA-256이나 SHAKE-256과 같은 안전한 해시 함수와 함께 구현될 수 있다. 이 스킴의 서명 및 검증 기능에서는 선택한 해시 함수가 스킴을 통해 처리된 전체 메시지나 파일에서 해시 값을 생성하는 데 사용된다. 이 해시 값은 메시지 다이제스트라고 불리며, 이후의 작업에서 서명을 생성하거나 검증하는 데 사용된다[3].

서명이 형성되는 방식으로 인해 키 생성 및 검증은 서명보다 훨씬 빠르다. SPHINCS+의 공개 키는 매우 짧지만 서명은 상당히 길게 생성된다.

SPHINCS+는 RSA 또는 Diffie-Hellman과 같은 수학적인 문제에 기반하는 가정 대신, 해시 함수의 중간값 충돌 저항성과 같은 특성에 의존하여 보안성을 제공한다. 그러나 구현 보안과 스킴의 보안 평가에는 복잡성이 영향을 미칠 수 있으며, 해시 함수의 내부 구조를 분석하는 것이 중요할 수 있다. 따라서 SPHINCS+를 사용하는 경우 선택한 해시 함수의 보안성과 구현 보안에 주의를 기울여야 한다.

3. Round 4 선정/비선정 알고리즘

본 단원에서는 NIST PQC 프로젝트의 Round 4에 진출한 Public-Key Encryption/KEMs 알고리즘들과 그렇지 않은 알고리즘들에 대해 더 자세히 탐구한다. Round 4에 선정된 알고리즘으로는 코드 기반 암호인 BIKE, Classic McEliece, HQC가 있고, 아이소제니 기반 암호 SIKE로 이들은 각각의 고유한 특성과 보안성을 기반으로 선정되었다. 반면, NTRU, SABER, Rainbow, FrodoKEM, NTRU Prime, GeMSS, Picnic은 다양한 이유로 Round 4에 진출하지 못했다.

<표 2>는 x86_64 프로세서 환경에서 다양한 PQC 후보 알고리즘들의 런타임 성능을 보여주는 표이다. 이 표에서는 키 생성, 암호화, 복호화의 연산 속도가 초당 연산 횟수로 표시되어 있다. KEM 알고리즘 중 BIKE와 HQC는 빠른 키 생성 및 캡슐화 속도를 보이는 반면, Classic McEliece와 같은 알고리즘들은 높은 캡슐화 및 복호화 속도를 가지고 있지만, 상대적으로 키 생성 속도가 현저히 느리다. SIKE와 NTRU는 균형 잡힌 성능을 보여주며, FrodoKEM은 중간 범위의 성능을 제공한다. Digital Signature 알고리즘인 Rainbow와 GeMSS는 더 긴 연산 시간을 요구하며, 이는 복잡한 수학 연산에 기인한다. Picnic은 매우 낮은 키 생성 속도를 보이지만, 상대적으로 빠른 캡슐화 및 복호화 속도를 나타낸다. 이러한 성능 차이는 알고리즘의 내부 연산 복잡성, 사용된 수학적 구조, 그리고 특정 암호 프로세스에 최적화된 구현 방식의 차이에서 비롯된다.

<표 2> x86_64 프로세서에서 알고리즘의 런타임 성능 분석[4]

알고리즘	키 생성/s	캡슐화/s	디캡슐화/s
BIKE-L1	4256.67	29602	1866.67
BIKE-L3	1345.33	14276.33	558
Classic McEliece-348864	7.2	55104.67	18448.67
Classic McEliece-460896	2.42	31683.67	7228.33
HQC-128	16412.33	9847.67	5710.67
HQC-192	7453.33	4283	2422.33
HQC-256	4232.67	2430	1435.33
SIKE-p434	98.8	60.57	56.52
SIKE-p751	92.91	57.49	53.45
NTRU-HPS-2048-509	14699	60072.3	71687.33
Saber-KEM	29017.7	29338.3	32348
FrodoKEM-640-SHAKE	794	669.11	719.76
Rainbow-I-Classic	6.77	506	500.7
GeMSS128	38.3 MC	736 MC	80.8 KC
Picnic-L1-FS	0.05	36.50	23.91

3.1 Round 4에 진출한 알고리즘

3.1.1 BIKE

BIKE는 코드 기반의 키 교환 메커니즘(KEM)으로 NIST 양자 내성 암호 표준화 공모전 Round 4의 후보 중 하나이다. 이 알고리즘은 다른 후보들과 달리 격자 기반 알고리즘이 아닌 오류 정정 코드의 수학적 성질을 활용하는 것이 특징이다. 특히 BIKE는 대역폭 측면에서 다른 후보 알고리즘들보다 상대적으로 작은 크기를 가지며, 이로 인해 데이터 전송 시 효율적인 성능을 보인다. 이는 BIKE가 대역폭 요구 사항을 줄이고 효율적인 통신을 가능하게 해준다.

BIKE는 QC-MDPC(Quasi-Cyclic Moderate Densit

y Parity-Check) 코드를 사용하며 디코딩 실패 확률에 대한 분석이 충분히 이루어지지 않아 보안성에 대한 주장이 완벽하지 않다[5]. QC-MDPC는 특정한 형태의 오류 정정 코드를 나타내며, 이 코드는 양자 컴퓨터에 대한 저항력을 가진 암호 시스템에 주로 사용된다. 이 알고리즘은 디코딩 실패율에 대한 추가적인 분석이 필요하며 NIST는 이러한 분석과 검증을 통해 BIKE의 보안성에 대한 신뢰를 높이기 위해 Round 4에 진출시켰다. 이는 BIKE의 잠재적인 취약점을 식별하고 해결함으로써 최종 표준화 과정에서 필요한 보안성을 확보하는 데 도움이 될 것이다.

3.1.2 Classic McEliece

Classic McEliece는 코드 기반의 KEM으로 CCA 보안을 달성하기 위해 이진 Goppa 코드를 사용한다. 그러나 공개 키의 크기가 크다는 점은 실제 사용에 있어 단점이 될 수 있다. 이는 통신 및 저장에서 비효율성을 초래하며 제한된 자원을 가진 시스템에서 특히 중요한 문제가 될 수 있다.

이 알고리즘의 잠재력을 최대한 활용하기 위해서는 추가적인 연구와 분석이 필요하다. 공개 키의 크기를 줄이는 방법, 보안성을 강화하는 기법, 실제 응용 프로그램에서의 효율적인 구현 방안 등에 대한 연구가 요구된다. 또한 양자 컴퓨터에 대한 저항성을 검증하기 위해 양자 알고리즘에 의한 공격 시나리오에 대한 철저한 분석이 필요하다. 이는 Classic McEliece가 양자 컴퓨팅 시대에서도 충분히 견딜 수 있는 보안 가정을 제공하는지를 평가하는 중요한 기준이 된다.

3.1.3 HQC

HQC는 BIKE와 유사한 방식으로 QC-MDPC 코드를 기반으로 한 KEM이다. 이 알고리즘은 강력한 보안성을 제공하며, 복호화 실패율에 대한 정확한 근사치를 제공한다. 또한 HQC는 코드의 숨겨진 구조를 복원하려는 공격에 강력한 면역성을 가지고 있다.

HQC의 준순환 구조는 공개 키와 암호문의 크기를 합리적으로 유지할 수 있도록 도와준다. 이는 통신 및 저장의 효율성을 향상시키는 장점을 가지고 있다. 그러나 다른 Structured 코드나 격자 기반 KEM에 비해 HQC는 약간 큰 공개 키와 암호문 크기를 가지고 있어 개선의 여지가 있다.

따라서 HQC는 전반적으로 합리적인 성능을 제공하지만, 향우 최적화를 위한 연구 개발에서 여전히 중요한 고려 사항으로 다루어질 것이다. 추가적인 연구를 통해 HQC의 성능을 개선하고 공개 키와 암호문의 크기를 줄이는 방법을 모색할 수 있을 것이다.

3.1.4 SIKE

SIKE는 공개 키 암호화와 키 교환에 사용될 수 있는 새로운 암호화 시스템이다. 그러나 최근 연구에 따르면 SIKE와 SIDH(Supersingular Isogeny Diffie-Hellman)는 취약점을 가지고 있다. SIDH는 아이소제니를 기반으로 한 공개 키 암호화 및 키 교환 메커니즘으로, 타원 곡선 간의 변환을 이용하여 양자 컴퓨터에 대한 저항력을 제공한다. 2022년 8월에 Castryck와 Decru가 게시한 논문[6]에서는 SIDH에 대한 효율적인 고전적 키 복구 알고리즘을 소개했다. 이 알고리즘은 SIKE에서 사용되는 특정 시작 곡선 값에 의존한다. 그러나 추가적인 연구에서 SIDH의 시작 곡선을 다양하게 변화시켜도 보안에 문제가 있다는 것이 밝혀졌다. 다른 연구자들이 결과를 통해 SIDH를 수정하는 다양한 방법을 제안했지만 이러한 수정은 SIDH의 성능과 키 크기에 부정적인 영향을 끼쳤다. 따라서 현재로서는 SIKE와 유사한 성능과 동시에 안전한 SIDH 변형은 알려져 있지 않다.

3.2 제외된 알고리즘

3.2.1 NTRU

NTRU[7]는 격자 기반 암호 알고리즘 중 가장 역사가 길고 오랜 시간 암호 분석을 통해 안전성을 검증받은 알고리즘이다. KYBER와 Saber와 같은 LWE 또는 LWR 기반 암호 시스템과는 다른 계산적 난해성 가정에 기반한다. 또한, NTRU는 소프트웨어에서 매우 우수한 성능을 보이지만 키 생성은 다른 두 격자 기반 후보들에 비해 상대적으로 느린 편이다. 대부분의 응용 분야에서 성능이 문제가 되지 않다고 했지만 NIST가 KYBER를 표준화로 선택했기 때문에 표준화로 고려되지 않았다.

3.2.2 SABER

다른 Structured Lattice KEMs와 마찬가지로, SABER[8]는 암호학적 연구의 큰 기반에 의해 지원되는 매우 효율적인 스킴이다. 그러나 NIST가 KYBER를 선택한 이유 중 하나는 NIST의 평가에 따라 KYBER의 대부분의 보안성을 설명하는 MLWE(Module-Learning With Errors) 문제가 SABER가 기반하는 MLWR (Module-Learning With Rounding) 문제보다 더 잘 연구되었다고 판단했기 때문이다[9]. 이 평가는 KYBER의 보안성 분석이 MLWE 문제에 대한 더 많은 연구와 이론적 기반을 가지고 있으며, 이는 KYBER의 안전성과 신뢰성을 높여준다.

3.2.3 Rainbow

Rainbow[10]는 다중 세그먼트 UOV(Unbalanced Oil and Vinegar) 구조를 사용하는 키 교환 알고리즘이며, 다변수 이차방정식을 기반으로 하는 디지털 서명 알고리즘(DSA)이다[11]. NIST PQC 표준화 과정의 후보 중 하나였지만, 매개 변수 선택에 대한 안정성이 부족하여 선정되지 않았다. 이 알고리즘은 다른 PQC 후보들에 비해 서명 크기가 작다는 장점이 있지만, 비용이 많이 드는 Tower Field-based 다항식 곱셈을 필요로 한다. 이는 특정 종류의 다항식 곱셈 방법으로, 일반적으로 높은 수준의 수학적 구조와 효율성을 필요로 하는 암호 알고리즘에 사용된다.

Rainbow에 대한 새로운 공격이 제시되었고, 이는 하이브리드 조합/대수적 공격 방법과 직사각형 MinRank 공격의 개선을 통해 Rainbow의 모든 매개 변수 세트의 보안 수준을 더욱 낮추었으며, Rainbow-I에 대한 공격이 실제로 가능해졌다. 이로 인해 이 알고리즘의 안정성과 신뢰성이 보장되지 않게 되었고, Round 4로의 진출이 이루어지지 않았다.

3.2.4 FrodoKEM

FrodoKEM은 LWE(Learning With Errors) 문제에 기반을 둔 KEM이다. IND-CCA 안전성을 세 가지의 레벨로 NIST가 정의한 보안 요구사항인 1/3/5이며 128/198/253 비트의 크기를 가졌다[12]. 이 알고리즘은 특히 평문이나 Unstructured-LWE 문제의 어려움에만 의존하여 설계되었으며, 이는 다른 LWE 기반 시스템들이 보통 Structured L:attice를 활용하는 것과 대조된다. FrodoKEM의 이러한 접근 방식은 특정 Structured Lattice를 기반한 알고리즘들이 가질 수 있는 잠재적 취약점에 대한 보안 이점을 제공할 수 있지만, 이는 동시에 계산 복잡성과 성능 저하를 초래할 수 있다.

NIST는 PQC 표준화 과정에서 BIKE, HQC, SIKE와 같은 다른 KEM 후보들이 FrodoKEM보다 더 적합하다고 판단하여 Round 4로 진행하지 않았다.

3.2.5 NTRU Prime

NTRU Prime[13]은 기존의 NTRU 암호 시스템을 변형하여 특정 공격에 대해 더 강력한 저항력을 제공하도록 설계된 알고리즘이다. 이는 기존 격자 기반 알고리즘들이 사용하는 대수적 구조와는 다른 새로운 링 선택을 통해 보안상의 이점을 추구하며, 이로 인해 NTRU, KYBER, SABER 같은 알고리즘들이 겪을 수 있는 보안 약화 문제를 줄일 수 있다고 주장한다. 그러나 이러한 주장에도 불구하고, NIST는 NTRU Prime을 표준화 후보에서 제외했다. 이는 NTRU Prime이 제시한 대수적 구조의 보안 이점에 대한 충분한 실증적 근거가 부족하다고 판단했기 때문이다. 결국, 이 결정은 대수적 구조에 기반한 공격에 대한 저항력과 관련하여, NTRU Prime의 주장이 충분히 설득력 있게 입증되지 않았음을 의미한다.

3.2.6 GeMSS

GeMSS[14]는 Feistel-Patarin 반복을 적용한 해시-서명 패러다임을 따르는 서명 스킴이다. 이 알고리즘은 Hidden Field Equation에 Vinegar 변수와 음수 값(HFEv-)을 기반으로 하는 트랩도어 함수를 사용한다. 대부분의 다항식 기반 스킴과 마찬가지로, GeMSS는 작은 서명을 생성하지만, 공개 키가 크고 서명 및 키 생성 작업이 상당히 느리다. 이 암호 분석은 Vinegar 변수와 음수 값이 HFEv-의 기본적인 설계 원칙을 약화시킨다는 것을 확인했다. 스킴을 복구하기 위해 변수와 음수 값을 포기하고 HFE 다항식의 차수를 높여 목표 보안 수준에 도달하거나 새로운 공격을 방지하기 위해 매핑이나 양수 값을 추가하는 등의 변경은 원래 제출된 암호화 체계에 큰 변화를 요구하며, 이로 인해

스킴의 성능이 받아들일 수 없게 되어 제외됐다.

3.2.7 Picnic

Picnic은 양자 컴퓨터에 의한 공격과 고전 컴퓨터에 의한 공격에 대한 보안을 제공하기 위해 설계된 서명 스킴이며, 영지식 증명 시스템을 사용한다. 이 알고리즘의 서명 속도는 SPHINCS+보다 빠르지만 검증은 느리다. NIST는 Picnic 대신 SPHINCS+를 선택한 이유 중 하나로 LowMC의 보안성에 대한 불확실성을 고려했다. LowMC(Low Multiplicative Complexity)는 경량 블록 암호 기반의 대칭 암호화 기법으로, 상대적으로 작은 키와 블록 크기를 가지면서도 높은 보안 수준을 제공하는 것을 목표로 한다. 하지만, 그 보안성에 대한 완전한 분석이 아직 이루어지지 않았으며, 현재로서는 충분한 이론적 또는 실질적 보안 증명이 제시되지 않았다.

5. 결 론

본 논문에서는 미국 NIST PQC 표준화 과정과 이 과정에서 선정 및 비선정된 알고리즘들에 대해 살펴보았다. NIST가 발표한 첫 번째 양자 내성 암호화 알고리즘 그룹은 주로 Structured Lattice와 해시 함수에 기반한 것으로, 이는 양자 컴퓨터에 의한 공격에 저항할 수 있는 고도의 수학 문제들을 해결함으로써 보안성을 제공한다. 현재 네 번째 라운드에서는 BIKE, Classic McEliece, HQC 알고리즘이 추가 검토 대상으로 남아 있으며, 이들은 각각 다른 보안 요구 사항 및 응용 프로그램에 적합한 다양한 기술적 접근 방식을 제공한다.

NIST는 2024년에 네 번째 라운드에서 선정된 알고리즘들과 현재 평가 중인 알고리즘들에 대한 다양한 측면을 논의하고, 최종적으로 어떤 알고리즘들이 표준화될 것인지에 대한 결정을 내릴 예정이다. 이 과정은 양자 컴퓨팅 시대에 대비한 공개 키 암호 시스템의 보안을 강화하고, 미래의 디지털 통신 시스템이 겪을 수 있는 위협으로부터 보호하기 위한 중요한 단계이다. NIST의 PQC 표준화 과정은 양자 컴퓨터에 대한 저항성을 갖춘 암호화 알고리즘을 개발하고 적용함으로써, 미래의 디지털 보안 환경에 중대한 영향을 미치는 역할을 수행할 것으로 기대된다.

양자 컴퓨팅 기술은 아직 초기 단계이므로 양자 공격의 실제 영향과 기능은 추측에 불과하다. 이로 인해 미래의 양자 위협에 대해 평가된 알고리즘의 견고성을 평가하는 것은 어렵다. 평가된 알고리즘의 기본 보안 가정은 현재의 수학적 이해를 기반으로 하였기에 예상하지 못한 잠재적인 취약점이 발견될 수 있다. 양자 컴퓨팅 기술이 발전함에 따라 발생할 수 있는 잠재적 취약점을 포함하여 양자 내성 알고리즘의 장기적인 보안 영향을 살펴볼 필요가 있으며, 양자 컴퓨팅으로 인해 디지털 보안에 제기되는 다양한 문제를 해결하기 위해 양자 내성 알고리즘 연구가 필요하다.

참고문헌

[1] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Ddang, J. Kelsey, J. Lichtinger, Y. K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, 'Status report on the third round of the NIST post-quantum cryptography standardization process', US Department of Commerce, NIST, 2022.

[2] 김규상, 박동준, 홍석희, "NIST PQC Round 3 FALCON 전자서명 알고리즘의 전력 분석 취약점 연구", 제31권, 제1호, pp.57-64, 2021.

[3] Duke-Bergman, Kei, A. Huynh, "Evaluating the performance of FPGA-based Secure Hash Algorithms for use in SPHINCS+", 2023 .

[4] Kumar, Manish, "Post-quantum cryptography Algorithms's standardization and performance analysis", Array, Vol. 15, 2022, 100242.

[5] 양유진, 오유진, 장경배, 서화정, "코드 기반 암호와 아이소제니 기반 암호의 공격 사례", 제33권, 제1호, pp. 51-58, 2023.

[6] Castryck, Wouter, T. Decru, "An efficient key recovery attack on SIDH", Annual International Conference on the Theory and Applications of

Cryptographic Techniques, Cham: Springer Nature Switzerland, pp. 423-447, 2023.
[7] NTRU, “https://ntru.org/f/ntru-20190330.pdf”, 2019.
[8] A. Basso, J. M. B. Mera, J. P D'Anvers, A. Karmakar, S. S Roy, M. V Beirendonck, F. Vercauteren, “SABER-Mod-LWR Based KEM (Round 2 Submission)”, 2021.
[9] V. B Dang, K. Mohajerani, K. Gaj, “High-speed Hardware Architectures and FPFA Benchmarking of CRYSTALS-Kyber, NTRU, and Saber”, IEEE Transactions on Computers, Vol. 72, No. 2, pp.306-320, 2022.
[10] Rainbow Round-2 Presentation, “https://csrc.nist.gov/CSRC/media/Presentations/rainbow-round-2-presentation/images-media/rainbow-ding.pdf”, NIST, 2019.
[11] 김광식, 김영식, “NIST PQC Rainbow의 효율적 유한체 연산 구현”, 정보보호학회논문지, 제31권, 제3호, pp. 527-532, 2021.
[12] 김예원, 염용진, 강주성, “GPU를 이용한 LWE 기반 양자 내성 암호의 병렬화 및 성능 분석”, 한국통신학회논문지, 제45권, 제12호, pp. 2183-2192, 2020.
[13] NTRU Prime, “https://ntruprime.cr.yp.to/nist/ntruprime-20201007.pdf”, 2020.
[14] A. Casanova, J. C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, J. Rycheghem, “GeMSS: A Great Multivariate Short Signature”, Diss. UPMC-Paris 6 Sorbonne Universites; INRIA Paris Research Centre, 2017.

〔저자소개〕

최 유 란 (Yu-Ran Choi)
2021년 3월 경남대학교 컴퓨터공학부 학사과정
email : yuran_@naver.com

최 윤 성 (Youn-Sung Choi)
2006년 2월 성균관대학교 정보통신공학부 학사
2007년 8월 성균관대학교 전자전기컴퓨터공학부 석사
2015년 8월 성균관대학교 전자전기컴퓨터공학부 박사
2016년 3월 ~ 2020년 2월 호원대학교 사이버보안학과 조교수
2021년 3월 ~ 현재 인제대학교 AI융합대학 조교수
email : cys2020@inje.ac.kr

이 학 준 (Hak-Jun Lee)
2015년 2월 한국교통대학교 소프트웨어공학 학사
2018년 2월 성균관대학교 전자전기컴퓨터공학 석사
2022년 8월 성균관대학교 전자전기컴퓨터공학 박사
2022년 9월~현재 경남대학교 컴퓨터공학부 조교수
email : hakjun@kyungnam.ac.kr