정 보 보 호 학 회 지
제 33 권 제2호, 2023. 4

양자컴퓨팅 환경에 안전한 암호로의 전환 동향

김 현 준*, 엄 시 우*, 송 민 호**, 서 화 정***

요 약

양자 컴퓨팅은 혁신적인 계산 패러다임으로, 큐비트를 사용하여 기존 슈퍼컴퓨터 상에서 복잡했던 문제들을 빠르게 해결할 수 있다. 다만 양자 컴퓨팅의 발전은 현대 암호의 보안성을 크게 위협함으로써 기존 암호화 시스템을 양자컴퓨팅에 안전한 암호화 시스템으로 전환하는 작업이 요구되고 있다. 현재 전세계 IT 기업들에서는 양자내성암호로의 전환과 관련하여 기존 암호 시스템과의 호환 그리고 새로운 암호의 보안성이라는 문제 해결을 위해 함께 연구 개발 중에 있다. 본 고에서는 양자컴퓨팅에 대비한 양자 내성 암호로의 전이 동향에 대해 조사하며 이와 관련된 문제, 전략 그리고 주요 고려 사항들에 대해 확인해 보도록 한다.

Ⅰ. 서 론

양자 컴퓨팅은 양자 역학 원리를 이용해 기존 컴퓨터에서 난제였던 것들을 해결가능할 것으로 기대되고 있다. 기존 컴퓨팅이 비트를 사용해 0과 1로 정보를 나타내고 있다면, 양자 컴퓨팅은 양자 얽힘과 양자 병렬성을 통해 0과 1 두 상태를 중첩하여 동시에 표현가능하다. 이러한 특성 때문에 양자 컴퓨터는 기존 컴퓨터보다 복잡한 계산을 빠르게 수행할 수 있다. 현재 양자 컴퓨터는 개발 초기 단계에 있으며, 복잡한 계산을 수행할 수 있는 대규모 양자 컴퓨터는 아직 상업적으로 이용할 수 없다. 그러나 전 세계의 연구자들과 기업들이 양자 컴퓨터 하드웨어와 소프트웨어를 개발하고 개선하기 위해 노력하고 있다.

양자 컴퓨터 개발의 주요 과제 중 하나는 환경에 매우 민감하며 작은 소음이나 간섭에도 쉽게 방해받는 큐비트의 안정성을 유지하는 것이다. 양자 컴퓨터 개발의 또 다른 과제는 양자 컴퓨터의 힘을 최대한 활용할 수 있도록 소프트웨어 도구와 알고리즘을 개발하는 것이다. 일반 컴퓨터는 다양한 소프트웨어 프로그램과 알고리즘을 실행할 수 있지만, 양자 컴퓨터는 양자역학 원리를 활용하기 위해 설계된 양자 알고리즘을 필요로 한다. 이러한 어려움에도 불구하고 최근 몇 년간 양자 컴퓨팅 분야에서 중요한 발전이 있었다. 2019년 구글은 "양자 우위"를 달성했다고 발표했다[1]. 여기서 말하는 양자 우위란 양자 컴퓨터가 일반 컴퓨터로는 사실상 해결 불가능한 문제를 해결할 수 있는 시점에 도달했음을 의미한다. 구글의 양자 컴퓨터는 세계에서 가장 강력한 슈퍼컴퓨터가 10,000년이 걸릴 계산을 200초 만에 수행할 수 있었다. 전반적으로 양자 컴퓨터 개발의 상태는 빠르게 진화하고 있다. 양자 컴퓨터가 더 강력해지고 널리 이용 가능해짐에 따라 복잡한 문제를 해결하고 다양한 분야의 과학 연구를 촉진할 것이다.

양자 컴퓨터가 더욱 강력해짐에 따라, 기업이 양자 내성 암호 알고리즘으로의 전이를 시작하는 것이 점점 더 시급해지고 있다. 이는 양자 컴퓨터의 공격으로부터 내성이 보장된 새로운 암호화 알고리즘으로 기존의 암호 시스템을 대체하는 것을 의미한다. 양자 내성 암호로의 전이에서 가장 큰 과제 중 하나는 기존의 암호 시스템이 금융 거래, 안전한 통신 및 정부 시스템 등 다양한 응용 분야에 깊이 프로그래밍되어 있다는 점이다. 이는 새로운 암호 시스템으로의 전이가 기존 응용

본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 50%) 그리고 본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 50%).

* 한성대학교 정보컴퓨터공학과 (대학원생, khj930704@gmail.com, shuraatum@gmail.com)
** 한성대학교 융합보안학과 (대학원생, smino0906@gmail.com)
*** 한성대학교 융합보안학과 (부교수, hwajeong84@gmail.com)

프로그램의 교란을 방지하고 새로운 시스템이 기존 응용 프로그램과 완전히 호환되도록 조심스럽게 계획되고 실행되어야 함을 의미한다. 양자 내성 암호로의 전이에서 또 다른 과제는 양자 내성 암호 알고리즘 개발과 관련된 여러 개방적인 질문과 과제들이 아직 많이 남아 있다는 점이다. 연구자들은 양자 컴퓨터의 공격으로부터 내성이 보장된 새로운 알고리즘 개발에 많은 진전을 이루었지만, 이러한 알고리즘들은 여전히 상대적으로 새롭고 실제 시나리오에서 완전히 테스트되지 않았다. 양자 내성 암호 알고리즘의 능력을 더욱 탐구하고 잠재적인 취약점과 약점을 식별하기 위한 연구 및 개발은 새로 개발되는 암호 시스템이 실제로 양자 컴퓨터의 공격에도 견딜 수 있는 것을 보장하기 위해 중요한 역할을 할 것이다. 본 고에서는 양자 내성 암호 전환 관련된 문제, 전략 및 주요 고려 사항에 중점을 두고 양자 내성 암호화 전이 동향을 조사한다.

Ⅱ. 양자 내성 암호

2.1. 현대 암호의 위기

양자 컴퓨터의 개발은 현재 고전 컴퓨터로는 풀기 어렵다고 여겨지는 수학적 문제에 의존하는 현대 암호학에 큰 위협이 되고 있다. 현대 암호화 시스템에 널리 사용되는 RSA 알고리즘은 큰 수를 소수로 분해하는 문제의 어려움을 기반으로 한다[2]. 그러나 1994년 Peter Shor가 개발한 양자 알고리즘인 Shor 알고리즘은 양자 컴퓨팅으로 큰 수의 인수 분해와 같이 기존 컴퓨터에게 계산이 많이 드는 작업을 효율적으로 수행한다[3].

양자 컴퓨터는 큰 숫자를 분해하는 것 외에도 타원 곡선 암호화 및 대칭 키 암호화와 같은 다른 유형의 암호화 알고리즘을 깨뜨릴 수 있는 잠재력을 가지고 있다. 양자 컴퓨팅의 또 다른 양자 알고리즘인 Grover 알고리즘은 정렬되지 않은 데이터베이스에서 값을 찾는 속도를 높일 수 있으며 이는 AES와 3DES 같은 대칭 키 암호 시스템을 깨는 데 걸리는 시간을 줄일 수 있다[4]. 또 다른 위협으로는 디지털 서명 및 기타 중요한 응용 프로그램을 보호하는 데 사용되는 SHA-2 및 SHA-3과 같은 해시함수에 대한 공격이다. Grover 알고리즘은 기존 컴퓨터보다 훨씬 짧은 시간 안에 해시 함수에서 충돌을 찾는 데 사용할 수 있다. 기존 암호 시스템의 보안에 대한 양자 컴퓨터의 위협은 양자 내성 암호 알고리즘에 대한 필요성을 강조하고 있다.

양자 컴퓨터가 더욱 강력해지면 RSA, ECC, AES와 같은 널리 사용되는 암호 알고리즘을 해독할 수 있게 되므로, 디지털 통신 및 저장된 데이터의 기밀성과 무결성이 저해될 수 있다. 이 위기를 해결하기 위해 연구원들은 양자 컴퓨터의 공격에 저항하도록 설계된 새로운 암호화 알고리즘을 개발하기 위해 노력하고 있다. 양자 내성 암호로 알려진 이러한 새로운 알고리즘은 양자 컴퓨터로도 풀기 어렵다고 여겨지는 수학적 문제에 의존한다.

2.2. 양자 내성 암호

양자 내성 암호학 또는 양자 이후 암호학은 양자 컴퓨터로부터의 공격에 대응할 수 있는 암호 알고리즘을 개발하는 암호학의 한 분야로, 양자 컴퓨터는 고전 컴퓨터보다 훨씬 빠르게 특정 수학 문제를 해결할 수 있다. 이 때문에 큰 수를 인수분해하거나 이산 로그 문제의 어려움에 기반하는 RSA 및 타원곡선 암호학과 같이 현재 널리 사용되고 있는 암호 알고리즘에 상당한 위협을 제기하고 있다. 이 잠재적 위협에 대응하기 위해 연구자들은 양자 공격에 저항할 수 있는 새로운 암호 알고리즘을 개발하고 있다. 양자 내성 암호 알고리즘은 고전 컴퓨터와 양자 컴퓨터 모두에게 어려운 것으로 여겨지는 수학적 문제를 기반으로 한다. 양자 내성 암호학에서 가장 유망한 연구 분야로는 격자 기반 암호학, 코드 기반 암호학, 다변수 암호학, 해시 기반 암호학, 아이소지니 기반 암호학이 있다.

격자 기반 암호학은 격자라는 기하학적 구조의 수학적 성질을 활용하며, 이는 복잡한 수학 문제를 해결하는 데 사용된다. Learning With Errors(LWE), Ring-LWE(RLWE), 그리고 NTRU와 같은 격자 기반 암호 체계가 있다[5, 6]. 코드 기반 암호학은 노이즈가 있는 채널을 통해 전송되는 데이터의 무결성을 보장하기 위해 에러 정정 코드를 기반으로 한다. McEliece암호 체계와 그 변형이 코드 기반 암호학의 대표적인 예이다[7]. 다변수 암호학은 다변수 다항 방정식 시스템을 해결하는 것을 포함한다. Unbalanced Oil and Vinegar(UOV) 및 Hidden Field Equations(HFE)는 다변수 암호 체계의 예이다[8, 9]. 해시 기반 암호학은 데이터를 거꾸로 복원하기 어려운 고정 길이의 출력으로 변환하는 해시 함수를 기반으로 한다. Merkle 서명

체계와 eXtended Merkle Signature Scheme (XMSS)이 해시 기반 암호 체계의 예이다[10, 11]. 아이소지니 기반 암호학은 타원곡선 및 도형, 특정 속성을 보존하는 타원곡선 사이의 지도와 같은 수학적 체계를 기반으로 한다. Supersingular Isogeny Diffie-Hellman (SIDH)과 Supersingular Isogeny Key Encapsulation (SIKE)은 아이소지니 기반 암호 체계의 예이다[12,13].

양자 내성 암호학은 여전히 활발한 연구 분야이며 'NIST 양자 내성 암호 표준화 프로젝트'와 같은 노력들이 양자 컴퓨팅 시대에 데이터와 통신의 보안이 계속 유지될 수 있도록 가장 안전하고 효율적인 양자 내성 암호 알고리즘을 식별하고 표준화하기 위해 진행되고 있다.

Ⅲ. NIST 양자내성암호 표준화 공모전

NIST(National Institute of Standards and Technology, 미국 표준 기술 연구소)에서는 양자 컴퓨터에 저항할 수 있는 새로운 암호 알고리즘을 개발하기 위해 양자 내성 암호(Post-Quantum Cryptography) 표준화 공모전을 진행하였다. 이 공모전의 주요 목표는 양자 컴퓨터의 발전에 따른 기존 암호 체계의 취약성을 극복하기 위해, 신뢰할 수 있는 포스트 양자 암호화 표준을 개발하는 것이다.

3.1. NIST 양자내성암호 표준화 공모전 진행 상황

NIST 양자 내성 암호 공모전은 2016년 시작되었으며, 여러 단계로 진행되고 있다. 참가자들은 양자 내성이 있는 공개키 암호화, 키 교환 및 디지털 서명 알고리즘을 제안하였다. 2017년 말 최초 제출 마감일까지 23개의 서명 방식의 암호와 59개의 공개키 암호/키 설정 방식의 암호가 제출되었다. 이 중 NIST의 기준에 맞는 69개(철회된 알고리즘 5개 포함)의 양자 내성 암호 알고리즘이 Round 1에 선정되었다[14].

2019년 1월 30일에 Round 2가 진행되면서 69개의 양자 내성 암호 중 발견된 공격법, 실용성 등의 문제로 여러 암호 알고리즘이 제외되었고 총 26개의 암호가 후보로 선정되었다[15]. Round 2에 선정된 알고리즘은 서명 방식 9개, 공개키 암호/키 설정 방식 17개로 이루어져 있으며, 격자 기반과 코드 기반의 문제를 어려움으로 하는 암호들이 주를 이룬다.

2020년 7월 22일 Round 3에서는 추가로 발견된 공격법, 실용성 등의 문제로 26개의 암호 후보 중 11개가 제외되었고, 7개의 Finalists와 8개의 Alternate가 선정되었다[16].

Finalists는 NIST 기준 Round 3 말에 표준화 준비가 될 것으로 예상되는 유력한 후보들이고, Alternate는 Round 3 이후에 선정 가능성이 있는 잠재적인 후보들이다. 2022년 7월 5일 최종적으로 표준 암호가 선정되었다. 선정된 알고리즘은 공개키 암호/키 설정 방식에는 격자 기반의 CRYSTALS-KYBER와 서명 방식에는 격자 기반의 CRYSTALS-Dilithium, FALCON, 해시 기반의 SPHINCS+가 있다[17].

표준 암호 선정 이후 추가로 진행된 Round 4는 공개키 암호/키 설정 방식에서 단일 알고리즘으로 선정된 CRYSTALS-KYBER 이외에 다른 알고리즘을 선정하기 위해 개최되었다[18]. 후보로는 코드 기반의 BIKE, Classic McEliece, HQC와 아이소지니 기반의 SIKE가 선정되었다. 이 중 유일한 아이소지니 기반인 SIKE는 공격법이 발견되어 제외되었다. 이후 진행된 네 번째 컨퍼런스에서 NIST는 서명 방식 중에 격자 기반이 아닌 암호들에 가장 관심이 많다고 하였으며, 표준 암호 선정 이유 및 표준화 목표를 전달하였다. 수많은 연구자들이 이 과정에 참여하여 포스트 양자 암호화 기술의 발전에 기여하고 있다.

3.2. 표준화 공모전 선택 알고리즘 비교

일반적으로, 암호화 알고리즘에서는 키의 크기가 클수록 보안 강도가 높아지는 경향이 있다. 그러나, 너무 큰 키 크기를 사용하면 성능이 떨어지거나 사용이 제한되는 문제가 발생할 수 있다. 따라서, 키 크기를 적절하게 조절하여 높은 보안 강도와 성능을 모두 만족시킬 수 있는 암호 알고리즘을 설계하는 것이 중요하다. 이러한 점에서, 적절한 키 크기를 사용하면서도 높은 보안 강도를 가진 양자 내성 암호 알고리즘은 잘 설계된 암호 알고리즘이라고 할 수 있다.

[표-1, 표-2]는 최종 선택된 양자 내성 암호 알고리즘과 4라운드에 올라온 알고리즘의 키 크기와 암호문 크기이다. [표-1]을 살펴보면, 최종 선택된 KYBER 알고리즘은 4라운드 후보 알고리즘과 비교하여 더 작은 공개키와 개인키 크기를 가진 것을 확인할 수 있다. 이렇게 암호화 알고리즘에서는 보안 강도 다음으로 키 길이와 성능이 중요한 척도로 고려된다. Classic

〔표 1〕 KEM 양자 내성 암호 알고리즘의 키 크기 및 암호문 크기(단위: Byte)

알고리즘	공개키	개인키	암호문
KYBER-512	800	1,632	768
KYBER-768	1,184	2,400	1,088
KYBER-1024	1,568	3,168	1,568
BIKE-L1	1,541	5,223	1,573
BIKE-L3	3,083	10,105	3,115
BIKE-L5	5,122	16,494	5,154
HQC-128	2,249	2,289	4,481
HQC-192	4,522	4,562	9,026
HQC-256	7,245	7,285	14,469
McEliece348864	261,120	6,452	128
McEliece460896	524,160	13,568	188
McEliece6688128	1,044,992	13,892	240
McEliece6960119	1,047,319	13,908	226
McEliece8192128	1,357,824	14,080	240

〔표 2〕전자서명 양자 내성 암호 알고리즘의 키 크기 및 서명 크기(단위: Byte)

알고리즘	공개키	개인키	서명
Dilithium2	1,312	2,528	2,420
Dilithium3	1,952	4,000	3,293
Dilithium5	2,592	4,864	4,595
FALCON-512	897	1,281	690
FALCON-1024	1,793	2,305	1,330
SPHINCS+-sha 256128s-simple	32	64	7,856
SPHINCS+-sha 256192s-simple	48	96	16,224
SPHINCS+-sha 256256s-simple	64	128	29,792

McEliece 알고리즘은 오랫동안 연구되어 안정성이 검증된 코드 기반 암호로 최종 선택 가능성이 높은 알고리즘이었다. 그러나, NIST에서는 이 알고리즘의 키 크기가 너무 크다는 이유로 널리 사용되기 어려울 것으로 판단하여 최종 선택에서 밀렸으며, 현재는 4라운드를 진행 중인 상황이다.

x86-64 프로세서를 사용할 때 Dilithium을 사용한 서명 생성은 FALCON보다 약간 더 빠르다. 그러나 데이터 전송은 이러한 체계를 사용하는 총 비용을 포함하므로 FALCON의 총 비용은 더 작은 공개 키 및 서명 크기로 인해 Dilithium의 총 비용보다 더 낮다[19].

이와 같이, 키 크기와 성능의 균형을 맞추는 것은 양자 내성 암호 알고리즘의 선택에서 중요한 고려사항 중 하나이다.

Ⅵ. 양자 내성 암호 전이 동향

암호 알고리즘은 취약점 발견, 종속 기술에 따른 제약이나 기술 발전으로 인해 교체되어야 한다. 특히 양자 컴퓨터의 발전으로 인해 현재 사용되는 많은 암호 알고리즘이 위협을 받고 있다. 양자 컴퓨터는 대부분의 전통적인 공개키 암호화 알고리즘을 빠른 시간 내에 해독할 수 있는 성능을 가지고 있어, 양자 내성 암호 알고리즘으로 전환하는 것이 필요하다. 그러나 많은 정보 시스템은 암호화 알고리즘을 빠르게 교체할 수 있는 높은 유연성을 갖추지 못하고 있다. 시스템 구성 요소에 따라 일부는 자주 교체되지만 다른 구성 요소는 수십 년 동안 사용될 것으로 예상된다. 암호화 알고리즘 교체는 시스템 구성 요소의 제약으로 인해 매우 어렵고, 경우에 따라 수십 년이 걸릴 것으로 예상된다.

NIST에서는 백서 Getting Ready for Post-Quantum Cryptography에서 표준화 프로세스가 완료된 후 양자 내성 암호화와 관련된 채택 문제 소개와 양자 내성 암호화로 마이그레이션하기 위한 계획 요구 사항에 대해 설명하였다 [20]. NIST의 백서에서는 양자 내성 암호화 표준이 구현 제약에 따라 다양한 애플리케이션에서 여러 알고리즘을 사용할 것으로 예상되며, 이러한 알고리즘 교체는 복잡한 과정으로 진행될 것이라고 설명하였다. 암호화 라이브러리, 검증 도구, 하드웨어, 운영 체제 및 애플리케이션 코드, 통신 프로토콜 등의 변경이 필요하며 이와 관련해 보안 표준, 절차, 모범 사례 문서도 수정하거나 교체해야 한다고 밝혔다. 또한, 알고리즘 교체를 계획할 때 체계적으로 각 요소를 고려하고, 영향 평가 및 호환성 검토를 수행하는 것이 중요하다고 강조하였다. 양자 내성 암호 알고리즘으로 이전할 때 고려해야 할 주요 사항은 다음과 같다.

양자 내성 암호 알고리즘으로 이전할 때 고려해야 할 사항은 구현이다. 양자 내성 암호 알고리즘은 상대적으로 새로운 기술로, 실제 상황에서 완전히 테스트되지 않았다. 다양한 양자 내성 암호 알고리즘의 보안성 및 신뢰성을 신중하게 평가하고, 취약점을 최소화하기 위해 올바르게 구현되도록 해야 한다.

양자 내성 암호 알고리즘으로 이전할 때 또 다른 고려 사항은 키 크기이다. 많은 양자 이후 암호 알고리즘은 기존 암호 시스템보다 더 큰 키 크기를 필요로 하며, 이로 인해 키 저장 및 전송에 어려움이 생길 수 있다. 양자 이후 암호 알고리즘을 선택할 때 보안과 실용성 간의 타협을 신중하게 고려해야 한다.

양자 내성 암호 알고리즘으로 이전할 때 또 다른 고려 사항은 성능이다. 많은 양자 내성 암호 알고리즘은 계산적으로 많은 처리량이 필요하며, 이로 인해 자원이 제한된 시스템에서 어려움이 발생할 수 있다. 양자 내성 암호 알고리즘을 선택할 때 보안과 성능 간의 타협을 신중하게 고려해야 한다.

양자 내성 암호 알고리즘으로 이전할 때 주요 고려 사항 중 하나는 기존 시스템 및 응용 프로그램과의 호환성이다. 많은 기존 암호 시스템은 금융 거래, 보안 통신, 정부 시스템 등 다양한 애플리케이션에 깊이 통합되어 있다. 새로운 암호 시스템으로의 이전은 신중하게 계획되고 실행되어야 하며, 기존 애플리케이션과 완전히 호환되는지 확인해야 한다.

마지막으로, 양자 내성 암호 알고리즘으로 이전할 때 고려 사항은 표준화이다. 많은 양자 내성 암호 알고리즘은 아직 개발 초기 단계에 있으며 표준화되지 않았다. 조직은 다양한 양자 내성 암호 알고리즘의 상태를 신중하게 평가하고, 표준화되고 널리 받아들여질 수 있도록 확인하여 다른 시스템 및 응용 프로그램 간의 상호 운용성 및 호환성을 보장해야 한다.

4.1. 구현 동향

4.1.1. 양자 내성 암호 알고리즘 구현 동향

[21]에서는 ARMv8 상에서 Falcon 최적화 구현을 제안한다. ARMv8에서 제공하는 NEON 엔진을 활용하여 최적화 구현을 진행하였다. Falcon의 핵심 연산 중 다항식 곱셈을 복소수 영역과 정수 영역을 최적화하는데 활용하였으며 FFT, NTT 기반 곱셈 방법을 개선하여 벡터 명령어를 적절히 활용한 병렬 구현을 제안한다. 또한 사용 가능한 레지스터를 최대한 활용함으로써 중복 메모리 접근을 최소화하였다. 이를 통해서 키 생성에서 15.1%, 서명 과정에서 16.5%, 검증 과정에서 65.4%의 성능 향상을 보여준다.

[22]는 Cortex-M4뿐만 아니라 Intel Haswell 상에서의 상수 시간 구현을 제안한다. 기존의 레퍼런스 구현 대비 디캡슐화 작업에서 1.39배의 속도 향상을 달성하였으며, 모든 작업을 포함하였을 때 1.33배의 속도 향상을 달성하였다. Barrel rotator 개념을 활용하고, 비트슬라이싱을 통해 합계를 계산하는 기법 등을 활용하여 최적화를 진행하였다.

[23]은 GPGPU를 활용하여 Dilithium 서명 알고리즘 최적 구현을 제안한다. 성능 향상을 위해 메모리 풀, 커널 융합, 배치, 스트리밍 등을 활용한다. 워프 수준의 디자인에 중점을 두고 CUDA 정수 내장 함수와 워프 수준 기본 요소를 활용하여 대규모 순차 작업의 병렬 계산을 가능하게 하였다. 이를 통해 낮은 IO 대기 시간과 높은 처리량을 달성하였다. 결과적으로 RTX3090Ti 환경에서 단일 스레드 CPU와 비교하였을 때, 키 생성, 서명 및 검증에 대해 각각 최대 57.7배, 93.0배, 63.1배 높은 처리량을 달성하였다.

4.1.2. 제한된 환경에서의 구현

NIST에서 양자 내성 암호 알고리즘을 설계할 때 필요한 사항으로 제한된 전력, 제한된 메모리, 스마트카드 그리고 8 비트 프로세서(예 : 음성 응용 프로그램, 위성 응용 프로그램 또는 기타 환경)를 포함하여 다양한 환경에서 알고리즘을 구현할 수 있는 능력도 평가 요소에 포함되어 있었다[24].

많은 PQC 알고리즘들은 저전력 마이크로컨트롤러용 ARMv7-M 아키텍처를 기반으로 하는 32-bit RISC 아키텍처인 Cortex-M4에서 최적화 구현이 진행되고 있다.

[25]는 Kyber와 Dilithium의 최적화 구현을 진행하였으며, 키 생성에서는 3.3-3.2%, 캡슐화에서는 3.1-3.6%, 디캡슐화에서는 5.1-5.2%의 성능 향상을 보여주고 있다. 이 구현은 높은 성능 향상을 위해 더 많은 스택을 사용하지만, 다른 구현물과 비슷한 스택 용량을 사용하여도 높은 속도 향상률을 보여주고 있다. 최적화를 위해 inverse NTT에 Cooley-Turkey를 사용하며, NTT 연산 과정에서 값을 캐싱하기 위해 부동소수점 레지스터를 사용하며, Kyber의 기본 곱셈에서 중복 계산을 제거하는 등 여러 다양한 기법을 적용하였다.

[26]은 Cortex-M4 상에서 Classic Mceliece의 상수 시간 구현을 제시하고 있다. 상수 시간 구현은 입력의

크기와 관계없이 결과를 계산하는데 걸리는 시간이 일정한 구현으로, 공격자가 입력 데이터의 크기를 바탕으로 정보를 추정하는 공격을 방지하는 구현 방법이다. Classic Mceliece는 Cortex-M4에서 제공하는 SRAM에 공개키를 저장하기에는 키 크기가 매우 큰 문제가 있다. 이를 해결하기 위해 플래시 메모리에 저장하여 사용한다. 또한, 비트 슬라이스 필드 곱셈 기법 등을 사용하여 연산 속도를 향상 시켰다.

4.1.3. Open Quantum Safe(OQS)

Open Quantum Safe (OQS) 프로젝트는 양자 컴퓨터 위협에 대응하여 안전한 암호화 표준 개발을 목표로 하는 오픈 소스 프로젝트이다[27]. 이 프로젝트의 목적은 양자 공격에 대한 내성이 있는 암호화 알고리즘 구현과 기존 암호화 시스템과 호환되는 방식으로 통합하기 위한 라이브러리 및 도구를 제공하는 것이다. OQS 프로젝트는 다양한 양자 내성 암호화 알고리즘 연구 및 개발을 수행하며, 이러한 알고리즘 중 일부는 이미 NIST의 양자 내성 암호화 표준화 과정에 참여하고 있다. 프로젝트는 인증서, 키 교환 및 디지털 서명과 같은 암호화 기능에 양자 내성 알고리즘 사용 방법에 대한 지침 및 예제도 제공한다. 이 프로젝트의 주요 결과물은 [표-3]과 같다.

〔표 3〕 프로젝트의 주요 결과물

결과물	설명
liboqs	오픈 소스 C 라이브러리로, 다양한 양자 내성 암호화 알고리즘 포함
OQS-OpenSSL	liboqs 라이브러리로, 기존의 OpenSSL에서 양자 내성 암호화 알고리즘 사용 가능
OQS-BoringSSL	liboqs 라이브러리로, 기존의 BoringSSL에서 양자 내성 암호화 알고리즘 사용 가능
OQS-양자 내성 암호 crypto-VPN	양자 내성 암호화 알고리즘을 사용하여 VPN 터널을 구축
OQS-KEMTLS	양자 내성 키 교환 매커니즘을 사용하는 TLS 프로젝트

Ⅴ. 호환 동향

5.1. NIST 양자 내성 암호 표준화 목표

NIST는 네 번째로 개최된 양자 내성 암호 표준화 컨퍼런스에서 최종 선정된 암호 알고리즘에 대한 표준화 목표를 밝혔다[28]. 보안 레벨 3, 4에 해당하는 KYBER-768과 KYBER-1024에 대해 표준화를 진행할 것이라고 확정했다. 보안 레벨 1에 해당하는 KYBER-512에 대해서는 토의가 진행 중이다. 보안성에 대한 걱정이 존재하나, 소프트웨어 측면에서 크기가 큰 KYBER-768 대신에 KYBER-512를 사용할 가능성이 있어 표준화 확률이 높다. 이외에 90S 버전은 표준화 목록에서 제외되었다.

CRYSTALS-Dilithium은 기본 서명 알고리즘으로 사용할 예정이다. 파라미터를 조정하여 보안 레벨 2, 3, 5에 맞출 것이라고 전달했다. 표준화 모델에서 AES 변형 모델인 Dilithium-AES는 제외되었다. Dilithium-AES는 Round 2에 대해 업데이트한 변형 모델로, 카운터 모드에서 SHAKE 대신 AES-256을 사용한다.

FALCON은 Dilithium과 같은 서명 방식의 격자 기반 알고리즘이지만, 어떤 어플리케이션에서는 Dilithium보다 구현이 복잡하며 비용적으로 효율적인 면이 있어서 선정되었다. 보안 레벨은 1, 5를 목표로 하고 있다. DIlithium의 완전 표준화 이후 FALCON에 대한 표준화가 진행될 예정이라 조금 늦어질 것이라고 전달했다.

SPHINCS+는 유일한 해시 기반 알고리즘이다. SHA-256를 사용하는 경우 보안 레벨은 1이며 SHA-256과 SHA-512를 같이 사용하는 경우엔 보안 레벨 3, 5이나, NIST는 사용할 해시 함수로는 SHAKE, SHA-256를 고려하고 있다고 전달했다. 표준화는 Round 1에 제출한 Robust 버전이 아닌 Simple 버전에 대해 진행된다. Simple 버전의 SPHINCS+는 Robust 버전에 비해 약 3배 정도 빠른 속도를 가지고

〔표 4〕 NIST의 보안 기준

Level	보안 설명
1	AES-128 깨기 어려운 정도
2	SHA-256 깨기 어려운 정도
3	AES-192 깨기 어려운 정도
4	SHA-384 깨기 어려운 정도
5	AES-256 깨기 어려운 정도

있다. 이외에 Fast 버전과 Small 버전도 표준화 목록에 포함된다.

5.2. 주요 프로토콜에서의 호환 동향

5.2.1. 하이브리드 키 교환

하이브리드 키 교환은 다양한 키 교환 알고리즘을 병합해 사용하며, 대부분의 구성 요소 알고리즘이 손상되어도 보안을 유지하는 것이 목표다. 많은 양자 내성 암호 알고리즘이 상대적으로 최근에 개발되어 RSA와 유한 필드 또는 타원 곡선 Diffie-Hellman만큼 연구되지 않았기 때문에, 보안 커뮤니티가 이들의 기본 보안성과 구체적인 보안 수준에 대해 완전히 확신하지 못하고 있다. 하이브리드 키 교환은 완전한 차세대 암호화 알고리즘 전환 전에 적절한 중간 단계가 될 수 있다.

5.2.2. 프로토콜 호환 동향

Transport layer Security(TLS)는 대칭키와 공개키 암호화 기술을 사용하여 통신 내용의 기밀성, 무결성, 인증 등의 보안 기능을 제공하며 인터넷에서 안전한 통신을 제공하기 위한 암호화 프로토콜이다. TLS는 Secure Sockets Layer(SSL) 프로토콜에서 파생되어 발전되었으며, 현재는 TLS 1.3 버전이 최신 버전으로 사용되고 있다. 양자 컴퓨터의 발전에 맞춰서 TLS에 사용되고 있는 암호화 알고리즘을 양자 컴퓨터로부터 안전한 양자 내성 암호 알고리즘으로 전환하는 연구가 진행 중이다.

[27]에서는 양자 컴퓨터로부터 안전한 공개키 암호 체계 설계에 대한 연구를 진행하였다.

[29]에서는 주요 인터넷 보안 프로토콜인 TLS와 SSH 프로토콜이 양자 컴퓨터가 양자 내성 암호 암호화를 적용할 수 있는지에 대한 연구를 진행하였다. 먼저 양자 내성 암호 및 하이브리드 키 교환 인증을 통합하기 위한 다양한 설계적 고려 사항을 검토하고 TLS 및 SSH에서 구체적으로 검토를 진행하였다. 하이브리드 암호화를 위해서는 여러 알고리즘의 사용과 여러 키를 결합하는 방법 등 여러 구현에 대한 연구가 진행되었다.

[30]에서는 양자 내성 암호 알고리즘의 사용화를 위해 TLS 1.3 아키텍처를 수정하여 양자 내성 암호 알고리즘을 안전하게 변형하여 사용할 수 있는 방법에 대해 연구를 진행하였다. ARM Cortex-M4 마이크로컨트롤러가 장착된 리소스가 제한된 임베디드 장치에서 양자 내성 암호 알고리즘이 적용된 PQTLS 1.3의 실행 시간, 메모리 및 대역폭 요구 사항에 대한 실험 결과를 제공하고 있다.

5.3. 미국 정부의 양자 내성 암호 전이

기존의 연방 및 상업용 기술과 암호화를 업그레이드하는 데 상당한 노력과 시간이 소요되기 때문에 양자 컴퓨팅 위협에 신속한 대응이 필요하다. 미국은 양자 컴퓨팅에 대한 사이버보안 대응을 개발하고 배치하는 전 세계적 노력에서 중요한 이정표가 되고 있다.

5.3.1. Commercial National Security Algorithm Suite 2.0

미국 국가안보국(NSA)은 Commercial National Security (CNSA) 문서를 발행하여 군사 및 정보 수집 활동과 관련하여 기밀 정보를 다루는 소유자, 운영자, 공급자가 사용해야 할 암호화 알고리즘을 명시한다. 지금까지는 CNSA 1.0이라고 불리는 기존 문서에 기반해 양자 저항이 반드시 보장되지 않은 고전적 암호화 알고리즘을 사용하였다. NIST가 3차 양자 저항 암호화(양자 내성 암호) 선택을 발표한 이후, NSA는 CNSA 2.0이라는 업데이트된 문서를 발표하고 어떤 알고리즘을 사용할지와 전환에 대한 예상 시간표에 대한 지침을 제공하였다.

CNSA 2.0에 현재 포함된 알고리즘은 대칭 블록암호 AES, 키교환 비대칭 알고리즘 CRYSTALS-Kyber, 디지털 서명 CRYSTALS-Dilithium, 정보의 축약 표현을 위한 계산 SHA, 펌웨어 및 소프트웨어에 대한 디지털 서명 LMS 과 XMSS이 있다. NSA는 사용 사례에 따라 2030년부터 2035년 사이에 완전한 전환을 완료하는 단계적 구현을 권장하였다.

5.3.2. OMB Memo Migrating to Post-Quantum Cryptography

미국 관리예산실(Office of Management and Budget, OMB)은 2022년 11월 18일 기관들이 양자 컴퓨터에 의한 재앙적인 공격으로부터 네트워크를 보

호하기 위해 취해야 할 조치에 대한 개요를 제시하였다. 기관들이 고가치 자산(HVAs)에 중점을 둔 현재의 암호화 시스템의 목록 작성과 같은 요구 사항이 포함되어 있다. 또한, OMB는 기관들에게 암호화 키와 연결을 생성하고 디지털 서명을 검증하도록 요청하였다. 기관들은 2023년 5월 4일 까지 OMB의 요청을 완료해야 한다.

5.3.3. H.R.7535 Quantum Computing Cybersecurity Preparedness Act

"연방 정부 기관이 양자 컴퓨팅 공격에 대비할 수 있는 기술을 채택하도록" 격려하기 위해 2022년 12월 21일, 바이든 대통령은 양자 컴퓨팅 사이버보안 대비 법안인 H.R.7535를 서명하여 법률로 만들었다. H.R.7535 법안은 연방 기관에 양자 컴퓨터와 표준 컴퓨터의 공격에 대비할 수 있는 후에 양자 내성 암호화로 시스템을 이전하도록 요구하였다. 이 법안은 양자 컴퓨터로 인해 약화된 암호화에 대한 위험에 대처하도록 연방 기관을 강제하였다. 2023년 5월까지 각 기관은 "양자 컴퓨터에 의해 복호화될 위험이 있는 기관에서 사용 중인 정보 기술의 현재 목록을 작성하고 유지"해야 한다는 법률 요건을 명시하였다.

Ⅵ. 결 론

본 고에서는 양자 내성 암호화 전이 동향을 조사하며 관련 문제, 전략 및 주요 고려 사항을 다루고 있다. 양자 컴퓨팅의 발전으로 기존 암호 알고리즘이 위협을 받아 양자 내성 암호 알고리즘으로 전환할 필요성이 대두되고 있다. 이러한 전환에는 구현, 키 크기, 성능, 호환성, 표준화 등의 고려 사항이 있으며, 다양한 양자 내성 암호 알고리즘과 프로젝트가 진행되고 있다. 미국 정부는 양자 컴퓨팅 위협에 대응하기 위해 전환 시기를 제안하고 법률로 제정하였다. 이를 통해 양자 컴퓨팅 시대의 데이터와 통신 보안을 유지하기 위한 표준화 노력이 필요할 것으로 사료된다.

참 고 문 헌

[1] Arute, Frank, et al. "Quantum supremacy using a programmable superconducting processor." Nature 574.7779, pp. 505-510, 2019.

[2] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2, pp.120-126, 1978.

[3] Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994.

[4] Grover, Lov K. "A fast quantum mechanical algorithm for database search." Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996.

[5] Peikert, Chris, "Lattice Cryptography for the Internet", IACR. Archived from the original on 12 May 2014.

[6] Stehle, D., and R. Steinfeld. "Making NTRUEnrypt and NTRUSign as secure as standard worst-case problems over ideal lattices." Cryptology ePrint Archive, Report 2013/004, 2013.

[7] Overbeck, R., and N. Sendrier. "Code-based cryptography, Post-Quantum Cryptography, ed. by DJ Bernstein, J. Buchmann, E. Dahmen." pp. 95-145, 2009.

[8] Bulygin, Stanislav, Albrecht Petzoldt, and Johannes Buchmann. "Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks." Progress in Cryptology-INDOCRYPT 2010: 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings 11. Springer Berlin Heidelberg, 2010.

[9] Patarin, Jacques. "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms." Advances in Cryptology—EUROCRYPT'96: International Conference on the Theory and Application of Cryptographic Techniques Saragossa, Spain, May 12–16, 1996 Proceedings 15. Springer Berlin Heidelberg, 1996.

[10] Merkle, Ralph Charles. Secrecy, authentication, and public key systems. Stanford university, 1979.

[11] Buchmann, Johannes; Dahmen, Erik; Hülsing, Andreas, "XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions". Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science. Vol. 7071. pp. 117–129, 2011.

[12] Costello, Craig, Patrick Longa, and Michael Naehrig. "Efficient algorithms for supersingular isogeny Diffie-Hellman." Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I 36. Springer Berlin Heidelberg, 2016.

[13] Jao, David, and Luca De Feo. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies." Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4. Springer Berlin Heidelberg, 2011.

[14] NIST, “Round 1 Submissions”, 2017, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions

[15] NIST, “Round 2 Submissions”, 2019, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[16] NIST, “Round 3 Submissions”, 2020, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

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

[18] NIST, “Round 4 Submissions”, 2022, https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

[19] Alagic, Gorjan, et al. “Status report on the third round of the NIST post-quantum cryptography standardization process”, US Department of Commerce, NIST, 2022.

[20] Barker, William, William Polk, and Murugiah Souppaya. "Getting ready for post-quantum cryptography: explore challenges associated with adoption and use of post-quantum cryptographic algorithms." The Publications of NIST Cyber Security White Paper (DRAFT), CSRC, NIST, GOV 26, 2020.

[21] YB Kim, JG Song and SC Seo. “Accelerating Falcon on ARMv8.” IEEE Access 10, 44446-44460, 2022.

[22] MS CHEN, T CHOU and M KRAUSZ. “Optimizing BIKE for the intel Haswell and ARM Cortex-M4.” Cryptology ePrint Archive, 2021.

[23] SHEN, Shiyu, et al. “High-Throughput GPU Implementation of Dilithium Post-Quantum Digital Signature.” arXiv preprint arXiv:2211.12265, 2022.

[24] NIST, “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”, 2016, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[25] Abdulrahman, Amin, et al. “Faster kyber and dilithium on the cortex-m4.” Applied Cryptography and Network Security: Proceedings. Cham: Springer International Publishing, 2022.

[26] MS CHEN and T CHOU. “Classic McEliece on the ARM cortex-M4.” IACR Transactions on Cryptographic Hardware and Embedded Systems, 125-148. 2021.

[27] Stebila, Douglas, and Michele Mosca. “Post-quantum key exchange for the internet and the open quantum safe project.” Cham: Springer International Publishing, 2017.

[28] NIST, “Fourth PQC Standardization Conference”, 2022,

https://csrc.nist.gov/events/2022/fourth-pqc-standardization-conference

[29] E CROCKETT, C PAQUIN, D STEBILA. “Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH.” Cryptology ePrint Archive, 2019.

[30] TASOPOULOS, George, et al. “Performance Evaluation of Post-Quantum TLS 1.3 on Resource-Constrained Embedded Systems.” Cham: Springer International Publishing, p. 432-451, 2022.

〈저 자 소 개〉

김 현 준 (Hyun Jun Kim)

학생회원

2019년 3월 : 한성대학교 IT응용시스템공학부 졸업

2021년 2월 : 한성대학교 IT융합공학부 석사 졸업

2021년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정

<관심분야> 암호화구현, 부채널분석

엄 시 우 (Si Woo Eum)

정회원

2021년 2월 : 한성대학교 IT융합공학과 졸업

2023년 2월 : 한성대학교 IT융합공학과 석사

2023년 3월~현재 : 한성대학교 정보컴퓨터공학 박사과정

<관심분야> 암호구현, 동형암호, 정보보호

송 민 호 (Min Ho Song)

정회원

2023년 2월 : 한성대학교 IT융합공학과 졸업

2023년 3월~현재 : 한성대학교 융합보안학과 석사과정

<관심분야> 암호구현

서 화 정 (Hwa Jeong Seo)

종신회원

2012년 2월 : 부산대학교 컴퓨터 공학과 석사 졸업

2016년 2월 : 부산대학교 컴퓨터 공학과 박사 졸업

2017년 2월~2023년 2월 : 한성대학교 IT융합공학부 조교수

2023년 3월 : 한성대학교 융합보안학과 부교수

<관심분야> 암호구현