NIST PQC와 KpqC 알고리즘 비교 분석

김명준, 서유진, 김영식
대구경북과학기술원
sanmaru98u@dgist.ac.kr, dmfive@dgist.ac.kr, ysk@dgist.ac.kr

Comparative Analysis of NIST PQC and KpqC Algorithms

MyeongJun Kim, YuJin Seo, Young-Sik Kim
DGIST

요 약

본 논문은 표준화를 거쳐서 선정된 양자내성암호(Post-Quantum Cryptography, PQC) 들을 비교 분석한다. 미국의 국립표준기술연구소(National Institute of Standards and Technology, NIST)에서 표준으로 선정한 알고리즘들과 대한민국의 양자내성암호연구단에서 선정한 알고리즘을 위주로 비교 분석하며 특히 실제 양자 내성암호 전환시 중요하게 고려해야 하는 파라미터의 크기를 비교하였다. 이에 따라 PQC 연구의 현주소와 향후 양자 내성 암호 전환 문제를 해결하는 연구 방향을 모색한다.

Ⅰ. 서 론

양자컴퓨터는 점점 현실이 되어가고 있다. 구글이 양자 오류 수정(quantum error correction)에 좋은 성능을 보이는 윌로우(Willow)를 발표한 이후, 마이크로소프트와 아마존에서도 양자 칩을 발표하였다.[1,2,3] 기존의 암호들은 소인수분해 또는 이산대수 문제 등을 기반으로 하고 있는데, 양자 컴퓨터를 이용한 쇼어 알고리즘(Shor's Algorithm)을 이용하여 이 문제를 다항 시간 안에 해결할 수 있을 것으로 전망하고 있다. 또한 그로버 알고리즘(Grover's Algorithm)으로 인해 기존의 해쉬암호도 위협을 받을 것이다. 즉, 기존의 표준 공개키 암호는 무용지물이 될 가능성이 크다고 판단됨에 따라 각 국가들은 양자컴퓨터에도 안전한 양자내성암호(Post-Quantum Cryptography, PQC)에 주력하고 있다.

현재 주요 국가들이 양자내성암호의 표준화를 진행하고 있다. 특히, 미국의 NIST의 암호 표준은 대부분의 국가가 자신들의 암호 설계에 중요하게 참고하거나 미국 표준을 그대로 채택하고 있다. 한국도 독자적인 양자내성암호 구축을 공모전 형태로 진행하였고, 한국 자체 PQC 알고리즘 4종을 최종 선정하였다.

본 논문은 미국과 한국을 중심으로하여 표준화에 선정된 PQC알고리즘들을 살펴보고, 그에 따른 의의와 향후 연구 방향을 모색하고자 한다.

Ⅱ. PQC 표준화

양자내성암호를 주도하는 미국 NIST 에서는 2016년 12월, 양자내성암호 표준화 공모전을 개최하여, 2025년 현재는 최근에 추가된 HQC를 포함하여 5개의 알고리즘을 선정하였다. 그 이후에도 격자 알고리즘에 대한 의존성을 낮추기 위해서 추가적인 전자서명 공모전을 진행중에 있으며, 현재 Round 2까지 진행된 상황이다. 본 장에서는 선정이 완료된 알고리즘에 한해, 전자서명과 키 캡슐화 매커니즘으로 분류하여 설명한다.

2.1 전자서명(Digital Signature)

CRYSTALS-DILITHIUM 기반 ML-DSA(Module-Lattice-Based Digital Signature Algorithm)와 FALCON 모두 격자 기반 암호이다. ML-DSA가 강력한 안정성을 보이고 있지만, 사이즈가 커서 적용이 불가능한 상황에서는 FALCON이 적절한 대체재가 될 수 있다[1,2,3]. 또한, FALCON은 향후 FN-DSA(FFT over NTRU-Lattice-Based Digital Signature Algorithm)로 NIST PQC 표준화될 예정이다. SPHINCS+에 기반한 SLH-DSA(Stateless Hash-Based Digital Signature Standard)는 격자 기반 암호에 과하게 의존하는 것을 피하기 위해서 선정되었으며 해쉬 기반 암호 형태를 취하고 있기에, 서명 크기가 큰 것이 특징이다. 또한, 각 파라미터 세트는 해시함수 계열의 SHA2 또는 SHAKE로 해시 함수가 생성이 되고, 해당 파라미터 세트가 상대적으로 작은 서명 생성('s')을 목표로 하는지 또는 더 빠른 서명 생성('f')을 목표로 하는지에 따라 scheme이 결정이 된다.[4]

표 1 ML-DSA, FALCON, SLH-DSA의 parameter에 따른 Security Level(SL), 서명, 키의 크기(Bytes)

Scheme	SL	공개키	서명	비밀키
ML-DSA-44	2	2,560	2,420	1,312
ML-DSA-65	3	4,032	3,309	1,952
ML-DSA-87	5	4,896	4,627	2,592
FALCON-512	1	897	666	1,281
FALCON-1024	5	1,793	1,280	2,305
SLH-DSA-SHA2-128s	1	32	7,856	64
SLH-DSA-SHAKE-128s				
SLH-DSA-SHA2-128f	1	32	17,088	64
SLH-DSA-SHAKE-128f				
SLH-DSA-SHA2-192s	3	48	16,224	96
SLH-DSA-SHAKE-192s				
SLH-DSA-SHA2-192f	3	48	35,664	96
SLH-DSA-SHAKE-192f				
SLH-DSA-SHA2-256s	5	64	29,792	128
SLH-DSA-SHAKE-256s				
SLH-DSA-SHA2-256f	5	64	49,856	128
SLH-DSA-SHAKE-256f				

한국의 경우, 2025년 1월 양자내성암호 국가공모전 최종 결과 발표를 통해 전자서명으로 HAETAE와 AIMer를 선정했다. HAETAE는 격자 기반 문제인 LWE 및 SIS의 모듈 버전 난제에 기초한 서명 체계며, "Fiat-Shamir with Aborts" 패러다임을 따르고 Rejection Sampling을 활용한다. 또한, HAETAE는 CRYSTALS-DILITHIUM과 유사하나,

Bimodal Distribution을 사용한 Rejection Sampling과 Hyperball uniform distribution에서 sampling하고 rejetcion하는 차이점이 있다.[5] AIMer는 특정 one-way function에 대한 preimage knowledge의 영지식 증명을 기반으로 하는 서명체계이며, BN++ 증명 시스템의 맞춤형 버전과 AIM one-way function 으로 되어있다.[6]

표 2 HAETAE와 AIMer의 parmeter에 따른 Security Level(SL), 서명, 키의 크기(Bytes)

Scheme	SL	공개키	서명	비밀키
HAETAE-120	2	992	1,474	1,408
HAETAE-180	3	1,472	2,349	2,112
HAETAE-260	5	2,080	2,948	2,752
AIMer-I	1	32	5,904	16
AIMer-III	3	48	13,080	24
AIMer-V	5	64	25,152	32

2.2 키 캡슐화 메커니즘(KEM)

미국의 경우, CRYSTALS-KYBER KEM의 3차 버전에서 파생된 ML-KEM이 NIST 선정 KEM의 유일한 알고리즘이였으나, Round 4에 존재하였던 HQC가 2025년 3월에 NIST에 의해 표준으로 선정되었다. ML-KEM은 MLWE를 기반으로 하여 빠른 속도와 작은 키 사이즈가 특징이며, HQC는 수십년간 안정성이 증명된 코드 기반 알고리즘이다.[7,8]

표 3 ML-KEM와 HQC의 parameter에 따른 Security Level(SL), 암호문, 키의 크기(Bytes)

Scheme	SL	캡슐화 키	역캡슐화 키	암호문
ML-KEM-512	1	800	1,632	768
ML-KEM-768	3	1,184	2,400	1,088
ML-KEM-1024	5	1,568	3,168	1,568
HQC-128	1	2,249	56	4,497
HQC-192	3	4,522	64	9,042
HQC-256	5	7,245	72	14,485

한국의 경우, NTRU+는 기존 NTRU 암호화 방식에서 단일 다항식으로 구성된 암호문의 간결한 구조와 공개 키 다항식의 계수를 sampling할 필요없이 더 빠른 암·복호화가 되는 장점과 함께 NTT(Number Theoretic Transform)에 최적화된 환 구조 활용 및 새로운 SOTP(Semi-Generalized One Time Pad) 인코딩 방법을 이용한다.[9]

SMAUG-T는 격자 기반 문제인, MLWE 문제를 활용하여 비밀키 보안을 강화하고 MLWR 문제를 활용하여 빠르고 효율적인 임시 키 생성을 제공한다. 또한, SMAUG-T는 PKE 체계인 SMAUG-T.PKE을 Fujisaki-Okamoto 변환을 통해 SMAUG-T.KEM으로 전환 후, IND-CCA2 보안을 가진다.[10]

표 4 SMAUG-T, NTRU+의 parameter에 따른 Security Level(SL), 키의 크기(Bytes)

Scheme	SL	캡슐화 키	암호문	역캡슐화 키
TiMER (IoT)	1	608	672	136
SMAUG-T128	1	672	672	176
SMAUG-T192	3	1088	1,024	236
SMAUG-T256	5	1792	1,472	218
NTRU+576	1	864	864	1,728
NTRU+768	1	1,152	1,152	2,304
NTRU+864	3	1,296	1,296	2,592
NTRU+1152	5	1,728	1,728	3,456

Ⅲ. 결론

본 논문은 2025년 현재 공식화된 미국 NIST PQC 표준 알고리즘과 국내 KpqC 표준을 비교 및 분석하였다. NIST는 FIPS 및 표준 사양 문서를 통해 계층별 보안 강도·시험 절차·검증 프로필을 명확히 규정하며, 연방정부 전체에 즉시 적용할 수 있는 정책적 구속력을 갖춘 반면, KpqC는 국산 알고리즘의 성능 및 경량 구현을 강조하고 산업계 자율 채택을 전제로 API·레퍼런스 코드·적합성 시험 가이드를 포함한다. 두 표준은 매개변수 선택(키 및 서명 길이), 인증·검증 체계 정책에서 차이를 보인다. 이러한 차이는 향후 글로벌 상호 운용성을 위해 상호 참조 시험 및 공동 벤치마킹이 필요함을 시사한다. 따라서, 각 국가는 표준화를 넘어 호환성 검증·전용 하드웨어 가속 등에 대한 연구를 서둘러야 한다. 이는 곧 다가올 양자시대에 국제 거래·공급망·디지털 서명 인프라가 단절 없이 연동될 수 있는 최소 요건이며, 궁극적으로 PQC 글로벌 표준의 수렴 및 상호 신뢰 체계 구축으로 이어질 것이다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(RS-2024-00399401, 양자안전 보안 인프라 전환 및 대양자 복합 안정성 검증기술 개발).

참 고 문 헌

[1] B.Y. Song “NIST 양자내성암호 표준화 현황,” 한국통신학회 동계종합학술발표회, 2024

[2] NIST, “Module-Lattice-Based Digital Signature Standard,” FIPS204, 2024

[3] Pierre-Alain Fouque, et al., “FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU,” submission to the NIST post quantum standardization process, 2020.

[4] NIST, “Stateless Hash-Based Digital Signature Standard,” FIPS205, 2024.

[5] J. H. Cheon, et al., “HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures,” Cryptology ePrint Archive, Paper 2023/624, 2023.

[6] S. Kim, et al., "AIM: Symmetric Primitive for Shorter Signatures with Stronger Security (Full Version)," Cryptology ePrint Archive, Paper 2022/1387, 2022.

[7] NIST, “Module-Lattice-Based Key-Encapsulation Mechanism Standard”, FIPS 203, 2024.

[8] C. Aguilar-Melchor, et al., “Hamming Quas-Cylic (HQC)”. Submission to the NIST post quantum standardization process, 2025.

[9] J. Kim and J. H. Park, “NTRU+: Compact Construction of NTRU Using Simple Encoding Method,” Cryptology ePrint Archive, Paper 2022/1664, 2022.

[10] J. H. Cheon, et al., "SMAUG: Pushing Lattice-based Key Encapsulation Mechanisms to the Limits," Cryptology ePrint Archive, Paper 2023/739, 2023.