NIST PQC Round 3 암호에 관한 성능 분석*

이명훈[1], 전찬호[1], 허동회[1], 김수리[2], 홍석희[3]

고려대학교 ([1]대학원생, [2]박사 후 연구원, [3]교수)

Performance Comparison of Round 3 candidates in the NIST PQC Standardization Project

MyeongHoon Lee[1], Chanho Jeon[1], Donghoe Heo[1], Suhri Kim[2], Seokhie Hong[3]

Korea University ([1]Graduate student, [2]Post Doc, [3]Professor)

요 약

양자컴퓨터가 개발됨에 따라 기존에 사용 중인 공개키 암호화 알고리즘 및 전자 서명 방식은 Shor's Algorithm에 의해 더 이상 안전하지 않다는 사실이 알려져 있다. 미국 국립 표준 연구소 (NIST) 에서는 양자 컴퓨팅 환경에서 안전한 양자 내성 암호 표준화 작업을 진행 중이다. 표준화 작업은 현재 round 3이 진행 중이며 후보 알고리즘은 7종으로 KEM (Key Encapsulation Mechanism) Classic McEliece, CRYSTALS-Kyber, NTRU, Saber 4종, 전자 서명 알고리즘 CRYSTALS-Dilithium, Falcon, Rainbow 3종이 있다. 본 논문에서는 NIST security category I 에 해당하는 보안 강도에서 round 3에 올라온 양자 내성 암호 후보 7종에 대해 Reference implementation 코드와 AVX2 implementation 코드의 알고리즘별 속도를 비교하고 향후 연구 방향을 제시한다.

I. 서론

컴퓨터의 계산능력이 향상됨에 따라, 향상된 컴퓨팅 환경에서도 안전하게 사용할 수 있는 암호가 요구되고 있다. 그 중, 양자컴퓨터 개발이 가시화된 현재 상황에서 양자컴퓨터가 실용화되면 기존에 사용중인 공개키 암호화 및 전자 서명 방식은 Shor's Algorithm [1] 에 의해 더 이상 안전하지 않다. 이에 대응하기 위해 양자 컴퓨팅 환경에서도 안전한 공개키 암호인 양자 내성 암호 (post-quantum cryptography, PQC) 가 필요해졌고, NIST에서는 2017년에 PQC 표준화 공모전을 시작하여, 현재 round 3이 진행 중이다.

양자 내성 암호는 기반 문제에 따라 크게 코드 기반 (Code-based) , 격자 기반 (Lattice-based) , 다변수 이차식 기반 (Multivariate-based) , 아이소제니 기반 (Isogeny-based) , 4가지로 분류할 수 있다. 이 중, round 3에는 1종의 코드 기반 암호인 Classic McEliece [2] 와 5종의 격자 기반 암호인 CRYSTALS-Kyber [3] , NTRU [4] , Saber [5] , CRYSTALS-Dilithium [6] , Falcon [7] 과 마지막으로 1종의 다변수 이차식 기반 암호인 Rainbow [8] 로 총 7종의 후보가 존재한다. 7종의 암호 중 KEM은 Classic McEliece, CRYSTALS-Kyber, NTRU, Saber로 4종, 전자 서명 알고리즘은 CRYSTALS-Dilithium, Falcon, Rainbow로 3종이다.

NIST에서는 위 7종의 알고리즘 중 KEM과 전자 서명 알고리즘 각각에서 양자 내성 암호의 표준 알고리즘을 선정할 예정이라고 공표했다.

본 논문에서는 NIST PQC round 3에 올라온 7종의 알고리즘 중 KEM 4종의 파라미터와 키 생성, 암호화, 복호화 수행 속도를 비교하고 3종의 전자 서명 알고리즘의 파라미터와 키 생성, 서명, 검증 수행 속도를 비교한다.

본 논문의 구성은 다음과 같다. 2장에서는 round 3에 올라온 7종의 알고리즘을 간략히 소개한다. 3장에서는 실험 결과를 통해 round 3에 올라온 KEM 4종과 전자 서명 알고리즘 3종의 파라미터 분석 및 수행 속도를 비교한다. 4장에서는 결론 및 알고리즘 개선 방향을 제안한다.

II. Round 3 후보 7종

본 장에서는 NIST PQC round 3에 올라온 후보 7종을 간략히 소개한다.

* 본 연구는 삼성전자의 지원(과제번호IO201209-07857-01)을 받아 수행된 결과임

2.1 KEM 4종

- *McEliece* : 선형 코드를 올바르게 디코딩 하는 것의 어려움에 기반하는 코드 기반 암호로, 이항 고파코드를 사용한다. 코드 기반 암호의 단점인 느린 복호화 속도를 보완한 알고리즘이다.
- *Kyber* : LWE (Learning With Errors) 문제에 대수적 구조를 더해 MLWE (Module-LWE) 의 어려움에 기반하는 격자 기반 암호로, 키 생성과 암복호화 과정이 빠르다는 장점이 있다.
- *NTRU* : 주어진 다항식을 작은 계수의 다항식 2개간의 나눗셈으로 표현하는 것의 어려움에 기반하는 격자 기반 암호로, 1996년에 제안돼 다른 격자 기반 암호에 비해 오랜 시간 암호학적으로 안전함이 검증되었다는 장점이 있다.
- *Saber* : LWR (Learning With Rounding) 문제에 대수적 구조를 더해 MLWR (Module-LWR) 의 어려움에 기반하는 격자 기반 암호로, 라운딩 과정에서 얻어지는 오차를 통해 안전성을 확보하므로 LWE기반 알고리즘에 비해 요구되는 연산량이 작은 알고리즘이다.

2.2 전자 서명 알고리즘 3종

- *Dilithium* : Kyber와 마찬가지로 LWE문제에 대수적 구조를 더한 MLWE의 어려움에 기반하는 격자 기반 암호로, Fiat-Shamir with abort방식을 사용하며 단순한 구현이 가능하고 키 생성, 서명, 검증과정이 빠르다는 장점이 있다.
- *Falcon* : NTRU격자 위에서의 SIS (Short Integer Solution) 문제의 어려움에 기반하는 격자 기반 암호로, hash-and-sign방식을 사용하며 다른 두 서명 알고리즘에 비해 공개키와 서명값의 크기 합이 작다는 장점이 있다.
- *Rainbow* : UOV (Unbalanced Oil and Vinegar) 문제의 어려움에 기반하는 다변수 이차식 기반 암호로, 공개키 크기는 크지만 서명의 크기가 작다는 장점이 있다.

III. 실험 결과

본 장에서는 NIST PQC round 3에 올라온 KEM 4종과 전자 서명 알고리즘 3종의 성능을 비교한다.

실험에 사용된 PC의 CPU는 Intel(R) Core (TM) i7-6700 CPU @ 3.40 GHz이며, 운영체제는 Ubuntu 20.04.1 LTS, 컴파일러는 GNU GCC version 9.3.0를 사용했다.

Table 1은 NIST PQC round 3에 올라온 알고리즘 7종을 KEM 4종과 전자 서명 알고리즘 3종으로 나눈 표이다. 단위는 파라미터 항목에는 바이트를 사용했고, 속도는 ms를 사용했으며 괄호 안에 적힌 숫자는 클럭 사이클을 의미한다. 실험한 알고리즘들은 NIST security category Ⅰ기준이며 Dilithium에 대해서는 category Ⅰ기준의 파라미터가 존재하지 않아 category Ⅱ기준에서 진행했다. 마지막으로, 각 알고리즘에 대해 구현 방법에 따라 reference implementation 환경과 AVX2 implementation 환경에서 실험을 진행했다.

3.1 KEM 4종 비교

- 파라미터 : 격자 기반 암호인 Kyber, NTRU, Saber의 암호문 크기는 768, 699, 736바이트인 반면, 코드 기반 암호인 McEliece는 암호문의 크기가 128바이트로 격자 기반 암호들에 비해 약 5배 이상 짧지만, 공개키, 개인키가 격자 기반 암호들에 비해 크다. 특히, 공개키의 크기가 261,120바이트로 가장 짧은 NTRU의 공개키 크기인 699바이트에 비해 약 373배 크다. 격자 기반 암호 내에서는 NTRU의 파라미터가 전반적으로 작은 경향을 보인다.
- 속도 : 키 크기가 큰 McEliece는 키 생성 속도가 다른 암호들에 비해 현저히 떨어진다. 특히, AVX2 implementation 환경에서도 키 생성 시간이 13.883ms이 소요되어 나머지 3종 중 가장 오래 소요된 0.203ms (NTRU의 키 생성 속도) 에 비해 약 68배 느리다. 격자 기반 암호 내에서는 Kyber의 키 생성 속도는 0.008ms이고 Saber의 키 생성 속도는 0.013ms로 0.203ms가 소요되는 NTRU보다 AVX2 implementation 환경에서도 10배 이상 빠름을 알 수 있다. 한편, 암복호화 속도는 4종의 알고리즘 모두 AVX2 implementation 환경에서는 0.05ms 이하의 속도를 보이는데 이 중 가장 느린 알고리즘은 NTRU이며 가장 빠른 알고리즘은 Kyber이다.

3.2 전자 서명 알고리즘 3종 비교

- 파라미터 : 격자 기반 암호인 Falcon, Dilithium에 비해 다변수 이차식 기반 암호인 Rainbow의 공개키는 161,600바이트로 Falcon의 897바이트에 비해 약 180배 크며 개인키는 103,648바이트로 Falcon의 1,281바이트에 비해 약 80배 크다. 반면, Rainbow는 서명의 크기가 66바이트로 Falcon의 666바이트에 비해 약 10배, Dilithium의 2,420바이트에 비해 약 36배 짧다는 장점을 가지고 있다. 전자 서명 알고리즘 중 파라미터 크기의 합이 가장 작은 알고리즘은 Falcon이다.
- 속도 : 키 생성 속도는 Dilithium이 AVX2 implementation 환경에서 0.03ms로 가장 빠르며 Falcon의 7.501ms에 비해 약 250배, Rainbow의 2.746ms에 비해 약 91배 빠른 속도이다. 하지만, 서명 속도는 Rainbow가 0.02ms로 Dilithium의 0.093ms에 비해 약 4배, Falcon의 0.229ms에 비해 약 11배 빠르며, 검증 속도는 Rainbow가 0.014ms로 Dilithium의 0.035ms에 비해 약 2배 Falcon의 0.044ms 비해 약 3배 빠르다. 파라미터가 상대적으로 작은 격자 기반 암호 Falcon과 Dilithium을 비교하면 Dilithium이 더 빠른 속도를 보여준다.

Table 1. Round 3 알고리즘 7종 파라미터 및 속도 실험 결과. 파라미터의 단위는 바이트이며. 속도의 단위는 ms이다. 단, 괄호 안의 숫자는 클럭 사이클을 의미한다.

구현 방법		Reference				AVX2			
KEM		*McEliece*	*Kyber*	*NTRU*	*Saber*	*McEliece*	*Kyber*	*NTRU*	*Saber*
파라미터	공개키	261,120	800	699	672	261,120	800	699	672
	개인키	6,492	1,632	935	1,568	6,492	1,632	935	1,568
	암호문	128	768	699	736	128	768	699	736
속도	키생성	97.644 (347,594,363)	0.033 (109,697)	24.014 (81,705,608)	0.021 (70,965)	13.883 (46,643,366)	0.008 (28,411)	0.203 (692,708)	0.013 (44,423)
	암호화	0.049 (169,560)	0.041 (139,305)	0.719 (2,453,306)	0.027 (92,961)	0.015 (53,926)	0.011 (37,389)	0.051 (173,456)	0.015 (53,007)
	복호화	19.445 (66,057,189)	0.049 (165,877)	1.879 (6,366,401)	0.031 (104,615)	0.035 (123,266)	0.008 (27,631)	0.032 (111,629)	0.014 (51,136)
전자 서명		*Dilithium*	*Falcon*	*Rainbow*		*Dilithium*	*Falcon*	*Rainbow*	
파라미터	공개키	1,312	897	161,600		1,312	897	161,600	
	개인키	2,544	1,281	103,648		2,544	1,281	103,648	
	서명	2,420	666	66		2,420	666	66	
속도	키생성	0.094 (306,687)	16.077 (55,331,852)	6.020 (20,561,806)		0.030 (102,199)	7.501 (24,239,478)	2.746 (8,804,507)	
	서명	0.436 (1,421,964)	4.589 (15,627,886)	0.075 (257,876)		0.093 (313,917)	0.228 (791,943)	0.020 (74,602)	
	검증	0.111 (363,506)	0.047 (156,081)	0.014 (47,324)		0.035 (119,420)	0.044 (151,819)	0.014 (53,823)	

IV. 결론

본 논문에서는 NIST PQC round 3에 올라온 알고리즘 7종의 NIST security category Ⅰ기준의 파라미터 및 속도를 분석했다.

KEM은 Kyber가 다른 알고리즘에 비해 전반적으로 작은 파라미터와 빠른 속도를 가지며 전자 서명 알고리즘은 Falcon이 작은 파라미터를 가지고 속도는 Dilithium이 가장 빠르다는 것을 확인했다.

알고리즘별로 안전성 및 최적화에 관한 연구가 끊임없이 진행되고 있으므로, 현 상황에서 단순히 속도가 빠르다고 하여 해당 알고리즘이 선택될 것이라는 보장은 없다.

향후에는, round 3에 올라온 7종의 알고리즘에 대해 어떤 연산이 코드에서 가장 큰 비중을 차지하는지 확인하고 안전성을 유지하며 해당 연산에서의 효율적인 연산을 통해 알고리즘 속도를 개선하는 추가 연구를 진행할 계획이다.

[참고문헌]

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

[2] M.R. Albrecht, et al., "Classic McEliece: conservative code-based cryptography," NIST PQC round 3 submission, Nov. 19, 2020.

[3] R. Avanzi, et al., "CRYSTALS-Kyber: Algorithm Specifications And Supporting Documentation," NIST PQC round 3 submission, Oct. 1, 2020.

[4] C. Chen, et al., "NTRU: Algorithm Specifications And Supporting Documentation," NIST PQC round 3 submission, Sep. 30, 2020.

[5] A. Basso, et al., "SABER: Mod-LWR based KEM(round 3 Submission)," NIST PQC round 3 submission, Oct. 21, 2020

[6] S. Bai, et al., "CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation," NIST PQC round 3 submission, Oct. 1, 2020.

[7] P.-A. Fouque, et al., "Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU: Specification v1.2," NIST PQC round 3 submission, Oct. 1, 2020.

[8] J. Ding, et al., "Rainbow," NIST PQC round 3 submission, Oct. 1, 2020.