NIST PQC 표준화 라운드 3 후보 알고리즘에 대한 임베디드 환경에서의 성능 비교

김광식, 김영식*

조선대학교 정보통신공학부

* 교신저자: iamyskim@chosun.ac.kr

Comparison of PQC Candidates in the NIST PQC Round 3 on an Embedded Computing Environment

Kwang-Sik Kim, Young-Sik Kim

Depart. Infom. & Commun. Eng., Chosun Univ.

요 약

본 논문에서는 현재 미국 NIST에서 진행 중인 3라운드 PQC 알고리즘 후보들에 대한 RaspberryPi Model B+상에서의 성능을 평가한 결과를 제시한다. 본 논문에서 사용한 SW는 2020년 4월에 저자들이 2단계 마지막 평가를 위해 갱신한 새로운 동작 코드를 기반으로 RaspberryPi 상으로 포팅하여 측정하였다. 이 논문은 PQC 알고리즘의 경량 환경에서의 성능 및 응용 방안에 대한 기초 데이터로 활용될 수 있을 것이다..

Ⅰ. 서 론

양자 컴퓨터 기술의 발전에 따라 양자 알고리즘을 통해 표준 공개키 암호 알고리즘을 해독하는 것이 현실적인 문제가 되고 있다. 양자 컴퓨터 기술은 국제적인 IT기업들의 주도로 빠른 속도로 발전하고 있으며, 최근에는 이미 특정한 문제에 대해서는 슈퍼컴퓨터의 성능을 뛰어넘은 것으로 평가되고 있다. 따라서 현재 널리 사용되는 RSA와 타원 곡선 암호(ECC) 기반의 암호화 및 전자서명 알고리즘을 해독할 수 있는 수준의 양자 컴퓨터가 10년 이내에 등장할 것으로 예상되고 있다.

이러한 문제에 대응하기 위해서 2017년부터 미국의 NIST에서는 포스트 양자 암호(Post-Quantum Cryptography) 알고리즘 표준화를 순차적으로 진행하고 있으며 2020년 7월에 3라운드 진출 알고리즘을 발표하였다 [1].

2라운드에서는 알고리즘의 성능을 중요한 지표로 사용하였지만, 대부분의 경우 PC상에서의 성능 분석을 위주로 진행되었고, 하드웨어 구현을 기반으로 한 성능 평가 결과들이 발표되고 있다 [2],[3]. 새로운 알고리즘은 앞으로 더욱 활성화될 사물인터넷 환경에서도 동작 가능해야하기 때문에 경량화된 연산 환경에서의 동작 성능을 평가하는 것이 중요하다.

본 논문에서는 현재 미국 NIST에서 진행 중인 3라운드 PQC 알고리즘 후보들에 대한 RaspberryPi Model B+상에서의 성능을 평가한 결과를 제시한다. 본 논문에서 사용한 SW는 2020년 4월에 저자들이 2단계 마지막 평가를 위해 갱신한 새로운 동작 코드를 기반으로 RaspberryPi 상으로 포팅하여 측정하였다. 이 논문은 PQC 알고리즘의 경량 환경에서의 성능 및 응용 방안에 대한 기초 데이터로 활용될 수 있을 것이다.

Ⅱ. NIST PQC Round 3 알고리즘

NIST에서 진행 중인 PQC 표준화는 처음에는 공개키 암호화, 키 캡슐화 메커니즘(KEM), 전자서명 세 가지 트랙으로 진행하였으나 3라운드에 이르러서는 공개키 암호화와 키캡슐화 메커니즘(KEM)이 합쳐져 총 두 개의 트랙으로 평가가 진행 중이다.

1단계는 NIST 일정에 따라 2017년 11월에 제안서 제출아 마감되었으며 총 67개의 알고리즘이 1라운드 평가 대상으로 선정되었고, 2019년 1월에 2라운드 진출 알고리즘으로 26개의 알고리즘이 선정되었다. 마지막으로 2020년 7월에 3라운드 알고리즘이 공개키 암호화 및 KEM 트랙에서 총 4개, 전자서명 트랙에서 총 3개의 알고리즘이 선정되었다. 표 1에는 NIST PQC 3라운드 진출 알고리즘을 종류별로 나타내었다.

표 1. NIST PQC 3라운드 진출 알고리즘

	Round 3		Alternatives	
	Algorithm	Category	Algorithm	Category
KEM	Classic McEliece	Code	BIKE	Code
	Crypstals Kyber	LWE	FrodoKEM	LWE
	NTRU	NTRU	HQC	Code
	Saber	LWR	NTRU Prime	NTRU
			SIKE	Isogeny
Digital Signature	Crystals Dillithium	LWE	GeMMS	MQ
	Falcon	NTRU	Picnic	Secret
	Rainbow	MQ	Sphincs+	Hash

표 1에서 나온 것처럼 3라운드 알고리즘은 총 7개로 추가로 8개의 알고리즘이 후보군으로 선정되어 향후 표준화에 선정될 수 있는 여지를 남겨두고 있다. 또 다른 특징으로는 각 부호들은 모두 서로 다른 카테고리에 속하는 것을 볼 수 있으며, 양자 연산의 안전성을 보장하기 위해서 알고리즘의 다양성을 최대한 유지하려고 하는 의도가 드러나고 있다.

3라운드 알고리즘은 향후 저자들에 의해서 수정을 할 수 있는 기회가 주어져 있기 때문에 2020년 내에 수정된 문서 및 알고리즘이 다시 한 번 더 제안될 예정이다. 따라서 현재로서는 3단계 수정본이 아닌 2단계 성능 평가를 위해서 저자들이 2020년 4월까지 수정한 코드르 대상으로 RaspberryPi 상에서의 성능을 평가하였다.

Ⅲ. Raspberry 환경에서의 구현 결과

본 논문에서 사용한 NIST PQC 3라운드 알고리즘에 대한 포팅 및 성능 평가는 일반적인 Raspberry Pi Model B+ 모듈을 사용하여 실시하였으며, 이 모듈은 1.4GHz의 동작 주파수를 갖는 64비트 Cortex-A53 (ARMv8)를 탑재하고 있으며, 1GB의 LPDDR2 SDRAM을 갖추고 있다. 운영체제는 Raspbian GNU/Linux 9.3를 사용하였다.

저자들이 작성한 코드는 표준 C를 사용해서 구현하기는 하였으나 외부 라이브러리 또는 OpenSSL 오픈소스를 사용해서 구현되었기 때문에, 이에 맞추어서 RaspberryPi 환경을 설정하고 실험을 진행하였다.

표준 C를 따르도록한 NIST의 가이드라인에도 불구하고 일부 알고리즘의 구현 코드들은 포팅 과정에서 수정이 필요하였으나, 공정한 비교를 위해 그 외의 부분은 저자들이 구현한 코들을 그대로 사용하였다. 또한 저자들이 제공한 테스트벤치인 KAT 파일을 통하여, 수정본의 정상적인 동작을 검증하였다. 이를 기반으로 한 시뮬레이션 결과는 표 2와 표 3에서 제시하였다.

표 2. NIST PQC 3라운드 KEM 알고리즘 성능 비교 (단위 ms)

Algorithms	Category	조건	Key Gen.	Encryption	Decryption
Classic McEliece	Code		N/A	N/A	N/A
Crystals-Kyber	MLWE	512	1.11	0.96	0.99
		768	1.97	1.66	1.69
		1024	2.62	2.46	2.48
NTRU	NTRU	509	65.01	1.84	4.83
		677	113.34	3.123	8.37
		821	166.58	4.48	12.21
		701	121.36	3.04	8.99
SABER	MLWR	114	0.85	1.17	1.23
		185	1.56	2	2.11
		257	2.48	3.04	3.2

표 3. NIST PQC 3라운드 전자서명 알고리즘 성능 비교 (단위 ms)

Algorithms	Category	조건	Key Gen.	Sign	Verification
Crystals-Dilithium	MLWE	Medium	2.39	6.62	1.78
		Recommended	2.72	9.49	2.73
		Very High	4.21	9.43	3.73
FALCON	NTRU	256	38.18	1547.21	198.25
		512	81.4	3203.04	406.24
		1024	343.96	6569.13	826.34
Rainbow	MQ	I	80.77	81.77	82.77
		I-Compress	87.83	46.88	15.05
		III	915.43	8.29	7.79
		III-Compress	990.6	522.68	87.97
		V	2729.87	16.83	17.86
		V-Compress	3036.16	1573.65	208.24

가장 오래된 PQC 알고리즘인 Classic McEliece의 경우 2라운드 진행중에 패리티 검사 행렬을 사용하는 Classic McEliece 알고리즘과 생성행렬을 사용하는 NTS-KEM 알고리즘이 결합해 Classic McEliece 알고리즘이 되었다. 그러나 오래된 만큼 저자들이 제공한 구현 코드는 RaspberryPi와 같은 경량 환경에서는 동작하지 않았으며, 동작을 위해서는 RaspbeeryPi 환경에 맞춰서 재설계가 필요하였다. 그러나 Crystals-Kyber나 SABER의 경우에는 경량 연산 환경임에도 불구하고 1ms내외의 동작 속도를 보여서 충분히 사물인터넷을 위해 이용가능한 것을 쉽게 확인할 수 있었다. 반대로 Rainbow 같은 알고리즘은 상대적으로 낮은 보안 수준의 경우 100ms 이내의 동작 성능을 보였지만, 보안 수준이 높아지면 응용이 어려울 것으로 예상된다.

Ⅳ. 결론

본 논문에서는 현재 NIST에서 진행중인 PQC 표준화 3라운드 선정 알고리즘들을 RaspberryPi라는 경량 환경에서 동작 성능을 평가하고 그 결과를 표로 제시하였다. 현재 3라운드가 마지막 라운드로 알려져 있으며 최종 알고리즘들이 12개월에서 16개월의 평가기간 후에 최종 발표될 예정이다. 향후 새롭게 업데이트되는 표준 알고리즘 상황에 맞추어서 실제 환경에서 응용 가능성을 평가하고 효율적이고 안전한 구현 코드로 확보하는 연구를 지속적으로 수행할 예정이다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원(IITP)의 정보보호핵심 원천기술개발사업인 “IoT 및 클라우드 컴퓨팅을 위한 경량 포스트 양자 암호 시스템 연구(R-20160229-002941)”의 연구결과로 수행되었음.

참 고 문 헌

[1] NIST, NIST PQC Round 3 Submisstions, https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions

[2] Banerjee, U., Ukyab, T. S., & Chandrakasan, A. P. (2019). Sapphire: A Configurable Crypto-Processor for Post-Quantum Lattice-based Protocols. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(4), 17-61.

[3] Albrecht, M. R., Hanser, C., Hoeller, A., Pöppelmann, T., Virdia, F., & Wallner, A. (2018). Implementing RLWE-based Schemes Using an RSA Co-Processor. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(1), 169-208.