양자 내성 암호의 기술개발 동향과 성능분석

최원석, 김영진, 임성묵, 정준시, 이슬기*
한국정보통신기술협회, *자율주행기술개발혁신사업단
wschoi@tta.or.kr, networker@tta.or.kr, seongmook.lim@tta.or.kr, jless@tta.or.kr, *sklee1014@kadif.kr

A Study on the performance of PQC (Post Quantum Cryptography)

WonSeok Choi, Youngjin Kim, Sungmook Lim, Joonsi Jeong, Seulki Lee*
Telecommunication Technology Association, *Korea Autonomous Driving Development Innovation Foundation

요 약

본 논문은 NIST에서 최근 발표한 양자 내성 암호화 4라운드에서 채택된 Crystals Kyber 알고리즘을 임베디드나 IoT 디바이스에서 널리 사용되는 ARM 기반의 CPU에서 구동하여 속도를 측정한다. 측정 결과를 기존 공개키 암호화 방식과 비교하고, 양자 내성 암호화 속도의 현재 상황을 확인한다. 양자 내성 암호의 확대 적용을 위해서는 고속화를 위한 하드웨어 기반의 가속 회로 설계 등의 연구가 수행되어야 전환이 가능할 것으로 보인다.

Ⅰ. 서 론

현재 인터넷, IoT 장치 등 다양한 분야에서 사용되는 공개키 기반의 암호화 알고리즘에는 RSA와 ECC가 대표적이다. RSA는 1978년, ECC는 1985년에 제안된 이래 가장 널리 사용되고 있는 알고리즘으로 각각 소인수분해와 무작위 타원곡선의 이산로그를 찾기 어렵다는 점을 이용하고 있다. 구현이 쉽고 암호화 속도가 빨라 널리 사용되었으나 1994년 Shor에 의해 고안된 인수분해 알고리즘이 양자컴퓨터를 이용하면 다항 시간 내에 가능하다고 제안됨으로써 안전성에 의문이 제기되게 되었다. 1996년에는 Grover 알고리즘이 제안됨으로써, 대칭키 암호화의 취약점을 보여주었다.

Ⅱ. 본론

본 논문에서는 Shor, Grover에 의해 취약점이 밝혀진 기존 암호화 알고리즘의 대응을 위해 개발된 양자 내성 암호(PQC: Post Quantum Cryptography) 기술개발의 최신 동향에 대해 살펴보고, 현재 구현된 양자 내성 암호의 성능을 분석하여 현재 상황과 발전 가능성을 제시한다.

미국 NIST에서는 2016년 차세대 암호 알고리즘 표준화를 목적으로 양자 컴퓨터에 안전한 암호화 알고리즘을 공모하기 시작하였다. 총 82개의 알고리즘이 접수되고, 1라운드로 64개의 암호화 알고리즘을 선정하였다. 다시 2라운드의 암호화 알고리즘 선정을 2019년 진행하여 26개의 암호화 알고리즘을 선정하였으며, 2020년 3라운드에서는 7개의 최종 후보 알고리즘과 8개의 대안 알고리즘을 선정하였다. 2022년 최종 4라운드를 거쳐 1종의 암호화 알고리즘과 3종의 전자서명 알고리즘을 선정하였고 해당 알고리즘에 대해 표준화를 시작하겠다고 발표하였다.

최종 암호화 알고리즘으로 선정된 Crystals Kyber는 격자기반의 암호화 알고리즘으로, Module-LWE, SIS 문제의 어려움에 기반을 두고 설계되었다. 다른 암호화 알고리즘에 비해 키 길이가 짧고 암호화 복호화 속도가 상대적으로 효율적으로 구현되어 현재 많이 사용되고 있는 암호화 알고리즘을 대체할 수 있을 것으로 기대되고 있다. Crystals Dilithium은 격자기반의 전자서명 알고리즘으로 Fiat-Shamir with aborts 구조를 따르고 있다. Falcon 알고리즘을 격자 기반의 NTRU 문제의 어려움에 기반을 두고 있는 전자서명 알고리즘이다. Crystals Dilithium 보다 키와 전자서명의 길이는 짧으나 전자서명 속도가 느리다는 단점이 있다. SPHINCS+는 해쉬 함수의 두 번째 역상을 찾는 문제의 어려움에 기반을 두고 있으며, 다른 난제 기반의 전자서명 알고리즘과 달리 단순하게 해시 함수 자체 문제의 어려움만을 요구하고 있어 알고리즘 측면에서 다른 방식보다 안전성이 높다. 그러나 서명의 길이가 매우 길고, 연산에서 약 45만 번의 해시 연산과 약 9만 번의 또 다른 해시 연산을 수행해야 하기에 다른 알고리즘보다 속도가 매우 느리다는 단점이 있다. 그러나 메모리의 대용량화, 프로세스의 고성능화로 SPHINCS+나 Falcon 등 다른 알고리즘도 지속적으로 개선이 이루어지고 있어 추후 다른 양자 내성 암호화 알고리즘보다 높은 성능을 제공할 가능성도 있다.

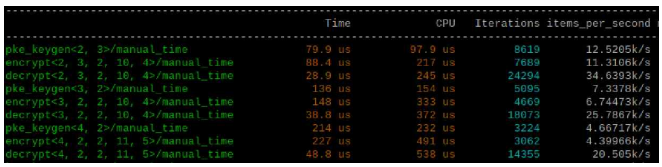
NIST에서는 양자 컴퓨터 시대 이후의 안전한 통신을 위해 크게 2단계의 전환 계획을 수립하고 있다. 1단계로 기존 공개키 암호화 알고리즘과 양자 내성 암호화 알고리즘을 동시 사용함으로써, 백워드 호환성을 달성하고 점차적으로 전환하는 기간을 의미한다. 2031년 이전까지의 기간으로 10년 정도의 기간을 1단계 하이브리드 전환 기간으로 계획하고 있다. 2단계 완전한 전환은 모든 분야에서 기존 공개키 알고리즘을 제거하고 양자 내성 암호로 전환하는 것을 의미한다. NIST에서는 1단계 이후 기간인 2031년 이후를 계획하고 있다. 본 논문에서는 Crystals Kyber 격자 기반의 암호화 알고리즘을 ARM 기반의 임베디드 환경에 포팅하여 성능을 측정하고 해당 암호화 알고리즘이 임베디드나 IoT 디바이스에서 적용 가능성을 분석한다. 기존 공개키 기반의 암호화와 비교하였을 때 성능 감소 폭을 확인하고 현재 상황에서 적용이 가능한 분야를 제시한다.

Crystals Kyber 알고리즘은 IND-CPA(공개키 방식)을 기반으로 하였으며, 32바이트의 메시지를 암호화하고, 다시 복호화하는 성능을 측정하였다. 공개된 Crystals Kyber 암호화 알고리즘은 ARM 기반의 CPU에서 컴파일 및 수행하는데 오류가 발생하여 소수점 연산 및 키 생성 부분, Thread

관련 부분을 수정하여 활용하였다. 암호화 알고리즘을 실행하기 위한 환경은 다음과 같다.

<표 1> Crystals Kyber 암호화 알고리즘 속도 시험환경

CPU	BCM2711B0 A72 (ARMv8-A)
Kernel	Linux kernel 5.15.61
Compiler Version	g++ 12.2
Memory	8GB LPDDR4-3200
Storage	micro SDXC 16GB UHS-I(U3)



<그림 1> Crystals Kyber 암호화 알고리즘 속도 시험모습

시험 결과 양자 내성 암호화 알고리즘인 Crystals Kyber는 32바이트 메시지 암호화 성능이 다음과 같이 측정되었다.

<표 2> Crystals Kyber 암호화 알고리즘 속도 시험결과

No	암호화 연산	Time(㎲)	초당 처리 속도(K/S)
1	PKE_KEYGEN <2, 3>	78.1	12.8054
	Encryption	88.1	11.3457
	Decryption	28.8	34.6826
	PKE_KEYGEN <3, 2>	135	7.43185
	Encryption	148	6.73683
	Decryption	38.9	25.7099
2	PKE_KEYGEN <2, 3>	78.4	12.7515
	Encryption	88.2	11.3408
	Decryption	28.8	34.7042
	PKE_KEYGEN <3, 2>	135	7.42164
	Encryption	148	6.73464
	Decryption	38.7	25.8169
3	PKE_KEYGEN <2, 3>	79.1	12.6439
	Encryption	89.0	11.2367
	Decryption	28.8	34.6646
	PKE_KEYGEN <3, 2>	137	7.32406
	Encryption	148	6.7406
	Decryption	38.9	25.7201
4	PKE_KEYGEN <2, 3>	79.8	12.5268
	Encryption	88.4	11.3111
	Decryption	28.8	34.6862
	PKE_KEYGEN <3, 2>	136	7.37956
	Encryption	149	6.7042
	Decryption	38.9	25.6885
5	PKE_KEYGEN <2, 3>	79.2	12.6216
	Encryption	88.3	11.3246
	Decryption	28.8	34.6952
	PKE_KEYGEN <3, 2>	136	7.36158
	Encryption	148	6.74267
	Decryption	38.8	25.7773

시험 결과 양자 내성 암호화 알고리즘인 Crystals Kyber는 32바이트 메시지 암호화 성능은 기존 AES-256이나 다른 암호화 알고리즘에 비해 반복 회수가 많아 매우 느림을 알 수 있었다. AES-256 대비 암호화 속도는 0.023% 정도이며 복호화 속도는 0.141% 정도로 측정되었다. 이는 암호화 속도의 경우 수천 배 느리며, 복호화 속도는 수백 배 이상 느림을 의미한다.

Ⅲ. 결론

본 논문에서는 NIST 양자 내성 암호화 알고리즘 4라운드에서 채택된 Crystals Kyber 암호화를 ARM 기반 CPU에서 수행하여 암복호화 속도를 확인하였다. 확인 결과 기존 공개기 암호화 방식에 비해 암호화 속도는 수천 배, 복호화 속도는 수백 배 느렸으며 이는 기존 공개키 기반의 암호화 방식을 당장 대체하여 적용하기는 어려움을 의미한다. 특히 임베디드 환경이나 IoT 디바이스 등에서 많이 사용되는 ARM 기반의 CPU에서는 더욱 느린 속도를 보여주었다. 이러한 느린 속도를 개선하기 위해 관련 가속 회로 등의 연구가 진행되어야 양자 내성 암호화 알고리즘으로 전환이 가능할 것으로 사료된다.

ACKNOWLEDGMENT

[이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2022-0-00979, 자율주행 차량 데이터 및 V2X 통신 네트워크 보안성 평가 기술 및 시험기준 개발)]

참 고 문 헌

[1] Davies R. W." Memory-Efficient High-Speed Implementation of Kyber on Cortex-M4 ,"AFRICACRYPT 2019, pp. 209-228.

[2] NIST, "Selected Algorithms," 2022, (https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022).

[3] 장세창, 하재철, "PQC 표준화 알고리즘 CRYSTALS-KYBER에 대한 비프로파일링 분석 공격 및 대응 방안," 정보보호학회논문지, pp.1045 - 1,057, Dec. 2022.