NIST 양자내성암호 공모전 Round2 코드기반암호 성능 비교 분석

장경배* 최승주* 권용빈* 김현지* 서화정*†

*한성대학교 IT융합과

Comparison of Round 2 Code-Based Cryptography for NIST Post-Quantum Cryptography Standardization

Kyoung-Bae Jang* Seung-Ju Choi* Yong-Bin Kwon* Hyun-Ji Kim* Hwa-Jeong Seo*†

*Division of IT Convergence Engineering, Hansung University.

요 약

미국 국립표준기술연구소 NIST (National Institute of Standards and Technology)에서는 양자내성암호 표준화 공모전을 개최하였다. 현재, Round1을 마치고 높은 평가를 받은 26개의 암호들이 Round2 평가에 돌입하였다. 본 논문에서는 후보 암호들에 대한 성능을 살펴보기 위해 코드기반 암호들에 대한 성능 평가를 2가지 대표적인 컴퓨팅 환경에서 진행한다. 해당 Round2 코드기반암호에 대한 성능 분석은 본 논문이 최초이며 이를 통해 Round3에 진출하게 될 알고리즘을 예상해 볼 수 있음과 동시에 현재 코드기반암호들이 개선해야 할 부분에 대해 심층 분석하도록 한다.

I. 서론

미국 국립표준기술연구소에서는 2016년 양자내성암호 표준화 계획에 대하여 발표하였고 세계 여러 각국에서 양자내성암호 알고리즘을 제출하였다. 표준화 후보들은 전부 NIST의 자체 보안 테스트를 통과하였기 때문에 안정성이 어느 정도 검증되었다고 볼 수 있다. 하지만 암호에 있어 보안성만큼 중요한 것이 암호의 성능이며 NIST의 표준화 공모전에서 매우 중요한 평가 요소이다. 이에 본 논문에서는 해당 코드기반 암호에 대한 성능 평가를 진행하였다. 현재 Round2를 진행 중인 17개의 공개키 암호 후보 중 7개가 코드 기반 암호로 많은 수를 차지하고 있다. 성능 평가 환경은 고성능 데스크톱 프로세서 Intel과 저전력 모바일 프로세서 ARM에서 진행하였다. 각각의 플랫폼에서 코드기반 암호 7가지의 키 생성, 암호화, 복호화 속도를 측정하였고 비교 분석해본다. 이를 통해 대부분의 양자내성암호가 공통적으로 갖고 있는 큰 키 크기의 문제, 연산 속도 등의 요소들이 각각의 환경에서 어떻게 작용되는지 알아본다. 또한 양자 후 시대에 암호들이 어떤 분야에 사용되는 것이 적합할지 평가해보고자 한다.

II. NIST 양자내성암호 공모전 코드기반암호 성능분석

양자 시대에 대비하기 위해서는 고성능 환경뿐만 아니라 저전력 환경에서도 반드시 양자내성암호가 적용 되어야 한다. 또한 암호의 성능은 사물인터넷 플랫폼과 같은 저전력 환경에서 더욱 중요하다. 이를 위해 NIST 코드기반암호 7가지를 다음 두 가지 환경 모두에서 실행해 본다. 각 암호의 키 생성, 암 복호화 속도를 비교해보고 이 암호가 어느 분야에 적용되면 적합할 것인지 분석해보고자 한다. 성능 평가 환경은 고성능 데스크톱 프로세서인 Intel 프로세서와 저전력 모바일 프로세서인 ARM에서 진행하였으며 100번의 Reference code 실행 후 평균 속도를 측정 하여 온라인에 결과물[1]을 게시하였다. 7가지 코드기반 암호 후보들의 특성과 성능을 비교 분석해보면 아래 Table 1와 같다.

	Code	Security history	Structure	Security level	Performance

1. https://docs.google.com/document/d/1075XjELMU_EsOFq_3fzvjEL-eu5Ud11ORZAI5mblYmM/edit

Classic McEliece	Goppa	long	KEM	IND-CCA2	low
BIKE	QC-MDPC	short	KEM	IND-CCA	high
NTS-KEM	Goppa	long	KEM	IND-CCA	low
HQC	QC	short	KEM	IND-CCA2	high
RQC	QC	short	KEM	IND-CCA2	high
ROLLO	Rank Metric	short	PKE/KEM	IND-CPA (KEM) IND-CCA2 (PKE)	high
LEDAcrypt	QC-LDPC	short	PKE/KEM	IND-CCA2	low

Table 1. Code-based Candidates comparison

기존 Goppa 코드의 사용을 고수하는 암호와 QC 시리즈, MDPC[1] 등의 새로운 코드로 대체하는 암호로 분류가 된다. Goppa 코드를 사용하는 암호들은 역사를 내세운 뛰어난 보안성을 강점으로 내세우지만 효율성이 떨어진다. Goppa 코드가 아닌 효율성이 좋은 새로운 코드에 기반 한 암호들은 성능이 Goppa 코드에 비해 비교적 높다. 하지만 검증된 기간이 길지 않기 때문에 지속적인 안전성 검증이 필요하다. 7가지 암호는 모두 기본적으로 KEM 버전을 제공하며 최소 IND-CCA의 보안레벨을 달성했다. 하지만 IND-CCA2의 보안레벨 달성을 위해선 사실 암호문에 해시 값을 추가하는 매우 비효율적인 과정이 필요하다. 성능 평가에서몇몇 IND-CCA2를 달성한 암호는 엄청난 성능저하가 발생한다. Intel 프로세서와 같은 고사양의 환경에서는 디바이스의 메모리 공간이 여유롭기 때문에 코드기반암호의 단점인 대규모의 큰 키를 수용할 수 있다. 이에 예상되는 적합한 구현 시나리오는 우선 키 생성, 배포비용에 투자를 해야 한다. 하지만 키 교환을 한번 수행하고 나면 개인키, 공개키 쌍은 오랜 기간 동안 배치될 수 있어야 한다. 따라서 코드기반암호 중 보수적인 Goppa 코드를 사용하여 키 생성 비용에 많은 투자가 필요하지만 상대적으로 준수한 암, 복호화 성능을 가지고 있는 Classic McEliece와 NTS-KEM이 적합해 보인다. 뛰어난 보안성을 자랑하기 때문에 양자 후 시대에도 안전하고 효율적인 통신이 가능할 것으로 보인다. 하지만 우려되는 분야는 저성능 환경이다. 성능평가 결과, ARM 프로세서 상에서 키 생성, 암호화/복호화 속도가 Intel 프로세서보다 약 10배 느리다. 그리고 암호의 효율성이 떨어질수록 이 10배의 수치는 더 크게 다가온다. 때문에 저사양 환경의 디바이스에 느린 속도의 암호를 탑재하기엔 무리가 있다. 이렇게 제한된 상황에 어떤 암호가 적합할지는 암호문을 얼마나 자주 교환하느냐가 매우 중요할 것이다. 주기적으로 잦은 통신이 필요하다면 우선 느린 암, 복호화 속도를 가진 후보는 고려해 볼 수도 없다. 저장 공간이 허용하는 선에서 안전하고 장기간 사용 가능한 키를 사용한 빠른 통신이 이상적이다. 하지만 여건이 충족되지 않는다면 ROLLO와 RQC와 같이 효율성을 중시한 코드기반암호가 최선일 것이다. 사실 코드기반암호를 이러한 환경에서 사용하기 위해선 QC시리즈 코드가 새롭게 등장하였듯 더 많은 연구가 필요하다. 혹은 코드기반암호가 아닌 보다 더 효율적인 다른 기법의 양자내성암호 선택도 고려해볼만 하다.

III. 결론

본 논문에서는 두 가지 환경에서 NIST 표준화 공모전의 코드기반암호에 대한 성능평가를 진행해 보았다. 각 암호의 특성과 성능의 관계에 대하여 분석해 본 결과, 이 두 가지 환경에서 조차 사용되기 적합할 암호들이 구분되었다. 하지만 실제로 더욱 다양한 환경의 디바이스가 존재하기 때문에 각 분야에 알맞은 양자내성암호가 필요할 것이다. 따라서 이번 NIST의 표준화 작업에선 하나가 아닌 여러 가지의 양자내성암호가 다양한 분야에서 각자의 특성에 맞게 표준화되어 활용될 것이다. 그리고 우리는 다가오는 이 양자 후 시대를 위한 NIST의 표준화 작업에 관심을 갖고 지켜봐야 하며 양자내성암호에 대한 지속적인 연구 또한 필요하다.

[참고문헌]

[1] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, Paulo S. L. M. Barreto, MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes , 2012.