NIST Round2 양자내성암호 공모전 코드기반암호 성능 비교 분석

최승주* 장경배* 김현지* 서화정*†

*한성대학교 IT융합

Performance Analysis of Code-Based Cryptography of NIST Round2 Post Quantum Cryptography Standardization

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

*Division of IT Fusion, Hansung University.

요 약

양자 컴퓨터의 시대가 현실로 다가옴에 따라 미국 국립표준기술연구소(National Institute of Standards and Technology, 이하 NIST)에서 양자내성암호 표준화 공모전을 개최하였다. 현재, Round1 평가를 거쳐 남은 26개의 암호들이 Round2 평가에 돌입하였다. 본 논문에서는 후보 암호 알고리즘 중 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 보며 현재 코드기반암호들이 개선해야 할 부분에 대해 분석을 진행하도록 한다.

I. 서론

미국 NIST에서는 다가오는 양자 컴퓨터 시대에 대비하기 위해 2016년 양자내성암호(Post-Quantum Cryptography) 표준화 계획안을 발표하였고 2017년 말 개최한 공모전에 세계 여러 각국에서 양자내성암호 알고리즘을 후보로 제출하였다. 제출된 후보들에 대해서 Round1에서는 보안성을 중점을 두고 평가를 하였고, Round2에서는 남은 후보군들에 대한 성능 등에 대한 기준을 토대로 평가가 진행되고 있다. 해당 표준화 후보들은 전부 NIST의 보안 테스트를 통과하였기 때문에 양자에 대한 내성의 안정성이 검증되었다고 볼 수 있다. 하지만 암호에 있어 보안성뿐만 아니라 암호의 성능 또한 중요하다. 이에 본 논문에서는 제출된 후보들에 대한 성능 평가를 진행하였고 대상은 코드기반암호이다[1-7]. 현재 Round2를 진행 중인 총 26개 중 17개가 공개키 암호 후보이며, 이중에 코드 기반 암호가 7개로서 많은 수를 차지하고 있다. 성능 평가 환경은 고성능 데스크톱 프로세서 Intel과 저전력 모바일 프로세서 ARM에서 각각 진행하였다. 각각의 플랫폼에서 코드기반암호 7개의 키 생성, 암호화, 복호화에 대한 속도를 측정하였고 비교 분석해본다. 분석 결과를 통해 양자내성암호가 공통적으로 갖고 있는 문제점인 큰 키 크기, 연산 속도 등의 요소들이 고성능 및 저전력 프로세서 환경에서 어떠한 성능으로 작용되는지 알아본다. 마지막으로 다가오는 양자 시대에 암호들이 어떤 분야에 사용되는 것이 적합할 것인지 평가해보고자 한다.

II. 양자 컴퓨터와 큐비트

양자 컴퓨터는 1980년대 컴퓨터에 양자 물리학을 적용하자는 아이디어를 제안하면서 등장하였다. 이와 같은 아이디어가 나온 당시에는 사람들의 큰 관심을 끌지는 못하였지만 1990년 대소인수 분해 양자 알고리즘이 제안되면서 이를 구현하려는 많은 연구가 진행되었다.

양자 컴퓨터와 기존 컴퓨터의 가장 큰 차이점은 연산을 진행하는 단위가 달라졌다는 점이다. 기존 컴퓨터는 0과 1중 하나로만 비트 단위

의 연산을 진행하였다면 양자 컴퓨터는 큐비트라는 단위를 사용한다. 큐비트는 기존 비트와는 다르게 0과 1이라는 상태를 동시에 가질 수 있으며 이러한 상태를 중첩이라고 부른다. 이러한 상태를 가질 수 있는 큐비트로 인해 표현할 수 있는 정보의 수가 기하급수적으로 늘어났고 많은 수의 큐비트를 활용하면 기존 컴퓨터로는 처리하지 못하는 정보의 양을 표현할 수 있게 될 것으로 예상된다. 또한 큐비트는 얽힘이라는 상태를 가질 수 있는데, 이는 하나의 큐비트의 상태를 측정하였을 때 해당 큐비트와 얽혀있는 상태로 연결되어 있는 다른 큐비트의 상태가 모두 단번에 결정되는 성질이다.

이와 같은 특성들을 활용해 기존 컴퓨터로는 수년의 시간이 걸려야 하는 연산을 중첩 상태의 병렬적 연산을 통해 단 몇 분 안에 처리할 수 있게 되었다. 대표적인 양자 연산으로는 소인수분해의 주기성을 찾는 문제로써 수학자 Shor가 제안한 Shor 알고리즘 등이 있다. 해당 알고리즘은 단 한 번의 연산만으로도 소인수분해에 필요한 지수 계산의 주기를 알아낼 수 있게 하는 양자 알고리즘이다.

이와 같은 연산 능력을 가진 양자 컴퓨터가 양산화가 된다면 현재 많이 쓰이고 있는 소인수분해 문제를 기반으로 한 공개키 암호화 알고리즘들은 사용할 수 없게 된다. 이미 양자 컴퓨터에 대한 개발은 많은 기업들이 개발 중에 있으며 구글에서는 53개 큐비트로 이뤄진 양자 컴퓨터를 개발했다 발표하였고 IBM에서는 20 큐비트 프소세서를 탑재한 양자 컴퓨터를 선보였다. 이와 같이 양자 시대에 양자 우위를 선점하기 위한 다양한 발전들이 이뤄지고 있는 상황이며 이와 동시에 양자 컴퓨터 시대에 대비한 움직임 또한 활발하게 진행되고 있다.

III. NIST 양자내성암호 공모전 코드기반암호 성능분석

양자 컴퓨터가 상용화 되는 양자 시대가 오면 많은 곳에서 사용되는 대표적인 암호 알고리즘인 RSA나 AES와 같은 암호 알고리즘들이 깨지게 된다. 이러한 상황은 해당 암호가 적용되는 분야 모든 곳에 영향을 미치게 된다. 이와 같은 상황에 대비하기 위해서는 고성능 환경뿐만 아니라 IoT 디바이스와 같은 저전력 환경에서도 반드시 양자내성암호가 적용되어야 한다. 특히 IoT 플랫폼과 같은 환경에서 암호의 성능은 매우 중요하다. 한정된 자원을 갖고 암호 연산을 진행해야 하는 플랫폼이기 때문에 암호 알고리즘에 대한 최적화가 필수로 필요해진다.

현재 제출되어 있는 NIST 양자내성암호 알고리즘 중 코드기반암호 7가지에 대한 현실적인 적용 가능성을 평가하기 위해 고성능 환경과 저전력 환경 두 가지 환경 모두에서 실행해 본다. 각 암호 알고리즘의 키 생성, 암호화, 복호화 속도를 비교해보고 각 암호가 어느 분야에 적용되면 적합할 것인지 분석해보고자 한다. 성능 평가 환경은 고성능 데스크톱 프로세서인 Intel 프로세서와 저전력 모바일 프로세서인 ARM에서 진행하였고 100번의 Reference code 실행 후 평균 속도를 측정 하여 온라인에 결과물[1]을 게시하였다. 7가지 코드기반 암호 후보들의 특성과 성능을 분석해보면 아래 Table 1과 같다.

	Code	Security history	Structure	Security level	Performance
Classic McEliece	Goppa	long	KEM	IND-CCA2	low
BIKE	QC-MDPC	short	KEM	IND-CCA	high
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
NTS-KEM	Goppa	long	KEM	IND-CCA	low

Table 1. Code-based Candidates Analysis

먼저 코드기반암호 중 가장 대표적인 암호 알고리즘인 McEliece와 같이 기존 Goppa 코드를 사용하는 암호와 QC, MDPC[1] 등 새로운 코드를 사용하는 암호로 크게 분류가 된다. Goppa

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

코드는 오랜 기간 사용된 코드로서 해당 코드를 사용함으로서 얻는 보안성에 대한 안전성을 장점으로 취할 수 있게 되나 효율성 부분에서는 좋지 못한 모습을 보여준다. Goppa 코드가 아닌 QC 시리즈의 코드를 사용하는 코드들은 비교적 성능이 Goppa 코드에 비해 높다. 하지만 해당 코드는 Goppa 코드에 비해 검증된 기간이 길지 않기 때문에 지속적인 보안성에 대한 검증과 증명이 필요하다. 코드기반암호 7가지 모두 KEM 버전을 제공하며 IND-CCA의 보안레벨을 달성한다. 더 높은 보안레벨인 IND-CCA2 정도의 보안레벨을 달성하기 위해서는 암호문에 해시 값을 연산하여 추가하는 매우 비효율적인 과정이 필요하다. 실제로도 성능 평가 과정 중에서 몇몇 IND-CCA2를 달성한 암호 알고리즘을 돌리는 도중 엄청난 성능 저하가 발생하는 것을 확인할 수 있었다.

Intel 프로세서와 같은 고사양의 환경에서는 디바이스의 메모리 공간 및 자원 등에 여유가 있었기 때문에 코드기반암호의 단점인 대규모의 큰 키에 많은 영향을 받지 않고 연산을 진행할 수 있다. 해당 환경에서는 키 생성, 배포에 자원이 더 할당되는 것이 좋을 것으로 보인다. 그러나 키 교환을 한번 수행하고 나면 개인키, 공개키 쌍은 오랜 기간 사용될 수 있어야 한다. 이에 코드기반암호 중 가장 오랜 역사를 갖고 있는 Goppa 코드를 활용하여 키 생성에는 자원이 많이 들지만 다른 암호 알고리즘에 비해 준수한 암호화 및 복호화 연산 성능을 보여주는 Classic McEliece와 NTS-KEM이 적합할 것으로 보인다. 높은 보안성을 자랑하기 때문에 해당 알고리즘들을 이용하면 양자 후 시대에도 안전하고 효율적인 통신이 가능할 것으로 보인다.

저성능 환경 같은 경우 성능평가 결과, ARM 프로세서 상에서 키 생성, 암호화/복호화 속도가 고성능 프로세서 환경보다 약 10배 느리다. 그리고 암호의 연산상의 효율성이 떨어질수록 해당 수치는 더 크게 영향을 끼치게 된다. 때문에 저사양 환경의 디바이스에 Classic McEliece와 같이 느린 속도의 암호를 탑재하기에는 적합하지 않을 것으로 보인다. 이와 같이 제한된 상황에서는 암호문을 얼마나 자주 교환하는지가 매우 중요할 것으로 보인다. 잦은 통신이 필요한 경우 느린 암호화, 복호화 속도를 가진 후보는 고려할 수 없다. 메모리 자원이 허용하는 한에서 안전하고 장기간 사용 가능한 키를 사용한 통신이 가장 적절할 것이다. 만약 이와 같은 조건이 만족되지 않는다면 ROLLO와 RQC와 같이 효율성을 중시한 코드기반암호가 현재로서는 최선의 선택일 것으로 보인다. 코드기반암호를 이와 같은 저전력 환경에서도 사용하기 위해서는 Goppa 보다 효율적인 QC시리즈 코드가 연구되었듯 앞으로 최적화에 대한 더 많은 연구가 필요할 것이다.

IV. 결론

본 논문에서는 고성능 환경 및 저전력 환경에서 NIST 표준화 공모전의 코드기반암호 7가지에 대한 성능평가를 진행하였다. 각 암호의 특성과 성능에 대하여 분석해 고성능 및 저전력 환경에서 사용되기 적합한 암호 알고리즘들 각각 구분하였다. 현실에는 더 많은 다양한 환경의 디바이스가 존재하기 때문에 각각의 환경에 맞는 양자내성암호가 필요할 것으로 예상된다. 그러나 NIST에서는 이번 공모전을 통해 하나의 표준만을 선출하는 것이 아닌 여러 가지의 양자내성암호가 다양한 분야에서 각자의 특성에 맞게 선출되어 활용될 것이라 밝힌바 있다. 해당 NIST의 표준화 공모전에 지속적인 관심을 갖고 지켜봐야 하며 양자내성암호에 대한 꾸준한 연구 또한 필요할 것으로 보인다.

[참고문헌]

[1] Daniel J, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Wen Wang, Classic McEliece: conservative code-based cryptography, 2019.

[2] Nicolas Aragon, Paulo S.L.M. Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, BIKE: Bit Flipping Key Encapsulation, 2019.

[3] Carlos Aguilar Melchor, Jean-Christophe

Deneuville, Nicolas Aragon, Philippe Gaborit, Slim Bettaieb, Edorado Persichetti, Hamming Quasi-Cyclic(HQC), 2019.

[4] Marco Baldi, Franco Chiaraluce, Gerardo Pelosi, LEDAkem: a post-quantum key encapsulation mechanism based on QC-LDPC codes, 2019.

[5] Carlos Aguilar Melchor, Philippe Gaborit, Nicolas Aragon, Adrien Hauteville, Magali Bardet, Ayoub Otmani, slim Bettalieb, Olieir Ruatta, ROLLO - Rank-Ouroboros, LAKE & LOCKER, 2019.

[6] Martin Albrecht, Carolos Cid, Kenneth G. Paterson, Cen Jung Tjhai, Martin Tomlinson, NTS-KEM, 2019.

[7] Carlos Aguilar Melchor, Alain Couvreur, Nicolas Aragon, Jean-Christophe Deneubille, Slim Bettaieb, Philippe Gaborit, Loic Bidoux, Adrien Hauteville, Oliveir Blazy, Gilles Zemor, Rank Quasi-Cyclic(RQC), 2019.

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