NIST PQC 공모전 동향 연구

이태호, 조영진, 박준우
한국정보통신기술협회
lth1124@tta.or.kr, choyj@tta.or.kr, junusee@tta.or.kr

A Study on the Trend of NIST PQC Contest

Lee Tae Ho, Cho Young Jin, Park Jun Woo
Telecommunications Technology Association

요 약

Shor의 알고리즘으로 인해 기존에 안전하다고 여겨져 온 다양한 공개키 암호들과 전자 서명 스킴들이 다항 시간 내에 쉽게 공격당할 수 있음이 알려졌고, 그 이후로 PQC(Post-Quantum Cryptography), QKD(Quantum Key Distribution) 등에 대한 연구를 통해 다양한 방면으로 미래에 생길 문제들을 대비하고 있다. 본 논문에서는 그러한 여러 노력 중에서도 NIST(National Institute of Standards and Technology)에서 진행하고 있는 PQC 공모전에 대한 동향을 소개한다. 국제 표준화 기구인 NIST는 앞서 진행되었던 AES, SHA3에 대한 공모전들과 같이 다양한 암호 알고리즘들의 신청과 등록을 받으며 효율성, 안전성, 구조 등에 대한 여러 방면에서 좋은 표준을 선정하기 위하여 1 라운드부터 3 라운드까지 진행하였으며, 현재는 추가 암호 알고리즘들에 대한 4 라운드를 통해 부족한 표준 암호 알고리즘의 수를 충당하고자 노력 중이다. 본 논문은 NIST에서 진행 중인 PQC 공모전에 대한 각 라운드에 관한 내용과 동향들을 소개하며 더 많은 관심이 필요함을 제시한다.

Ⅰ. 서 론

1994년 Shor의 알고리즘이 제시된 이후 양자 컴퓨터가 개발되면 양자 알고리즘을 이용하여 현재 존재하는 이산 대수 기반, 소인수분해 기반의 어려움을 가지는 공개키 암호 체계들과 전자 서명이 다항 시간 내에 분석됨이 알려졌다[1]. 이는 통신에서 매우 중요한 알고리즘들로 키 교환, 비밀정보 교환 등의 공개키 특성을 이용하여 편리하게 사용했던 것들이 안전성의 큰 문제를 가지게 될 것이라는 전망을 의미하였다. 이후, 다양한 암호 알고리즘들과 QKD 등 다양한 방면으로 연구가 진행되었고 그중에서도 본 논문은 NIST에서 진행하고 있는 양자 내성 암호 PQC 공모전에 대한 동향을 소개한다. NIST는 2016년에 PQC에 대한 리포트를 제시하며[2], 공모전에 대한 소개를 진행하였고, 이후 2017년 1 라운드, 2019년 2 라운드, 2020년 3 라운드를 거쳐 2022년에 드디어 표준 암호들을 선정하였으며 현재는 추가 암호들에 대한 4 라운드를 진행하고 있다.

Ⅱ. 1 라운드

2017년 12월, NIST PQC 공모전에 [표 1]과 같이 격자 기반 어려움 등을 난제로 기반하는 다양한 PQC 후보들 64개(철회된 알고리즘 5개 제외)가 1 라운드에 등록되었다[3].

〔표 1〕 NIST PQC 1 라운드 암호 알고리즘 통계

Round 1	전자 서명	KEM/ENC	**총계**
격자 기반	5	21	**26**
코드 기반	2	17	**19**
다변수 기반	7	2	**9**
대칭/해시	3	-	**3**
기타	2	5	**7**
총합	**19**	**45**	**64**

이후, 2018년 4월 첫 번째 PQC 표준화 컨퍼런스가 개최되었고, 해당 컨퍼런스에서는 후보로 등록된 다양한 암호 알고리즘들에 대한 소개와 구조들을 개발자들이 설명하였다[4]. 기존 1 라운드 69개(철회된 알고리즘 5개 포함) 중 21개는 해당 컨퍼런스가 개최되는 4월 전에 공격법들이 발견되었다.

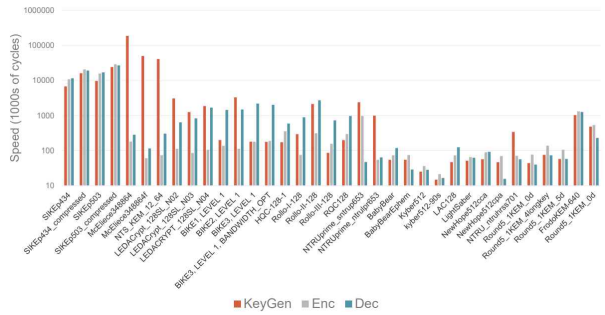
Ⅲ. 2 라운드

2019년 6월, NIST PQC 공모전에 [표 2]와 같이 1 라운드 후보 64개의 PQC 후보 중 38개가 효율성, 알려진 공격법, 그리고 구조 등에 의한 문제들로 탈락하였고, 총 26개의 암호 알고리즘만이 후보로 등록되었다[5]. 해당 알고리즘들은 주로 격자 기반과 코드 기반의 문제를 어려움으로 하는 알고리즘들이다.

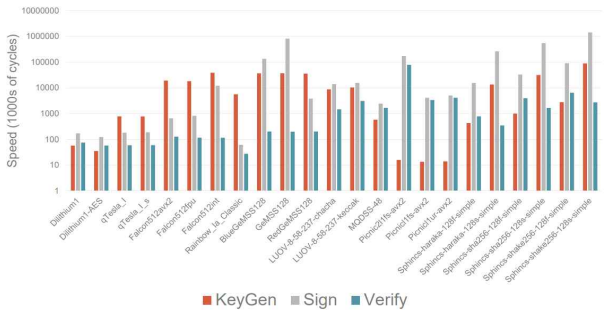
〔표 2〕 NIST PQC 2 라운드 암호 알고리즘 통계

Round 2	전자 서명	KEM/ENC	**총계**
격자 기반	3	9	**12**
코드 기반	-	7	**7**
다변수 기반	4	-	**4**
대칭/해시	2	-	**2**
기타	-	1	**1**
총합	**9**	**17**	**26**

이후, 2019년 8월에 두 번째 PQC 표준화 컨퍼런스가 개최되어 1 라운드로부터 2 라운드로 넘어가는 과정에 대한 것과 각 암호 알고리즘들의 2 라운드 변경점, 산업에서의 응용 방안 등을 위주로 발표가 이루어졌다[6]. 아래 [그림 1]과 [그림 2]는 컨퍼런스에서 Opening Remarks로 발표된 "The 2nd Round of the NIST PQC Standardization Process-Opening Remarks at PQC 2019"에 있는 자료로 2 라운드 후보들의 속도를 각 알고리즘의 핵심 연산마다 비교한 것이다.



〔그림 1〕 2 라운드 KEM/ENC에 대한 속도 비교



〔그림 2〕 2 라운드 전자 서명에 대한 속도 비교

특히, 해당 발표에서는 각 암호 알고리즘들에 적용된 수학적 안전성에 대한 증명들뿐만 아니라 Cortex M4와 Artix-7에서의 효율성(시간, 크기 등)을 강조하였고, 무엇보다도 부채널 분석에 관해 얘기하며 안전하게 구현하는 것을 중요하게 볼 것이라고 전달하였다.

Ⅳ. 3 라운드

2020년 7월, NIST PQC 공모전에 [표 4]와 같이 2 라운드 후보 26개의 PQC 후보 중 11개가 효율성, 추가로 알려진 공격법 등에 의한 문제들로 탈락하였고, 총 7개의 Finalists 후보들과 8개의 Alternates 후보들 총 15개의 암호 알고리즘만이 후보로 등록되었다[7]. 이 중에서 Alternates 후보들은 Finalists 후보들에 문제가 생기면 대체 하는 방안으로 존재하는 것들이다. 후보들 대부분은 격자 기반의 어려움을 토대로 하고 있어 가장 표준이 되기에 우세한 후보들이라고 생각할 수 있다.

〔표 3〕 NIST PQC 3 라운드 암호 알고리즘 통계

Round 1	전자 서명	KEM/ENC	**총계**
격자 기반	2(-)	3(2)	**5(2)**
코드 기반	-	1(2)	**1(2)**
다변수 기반	1(1)	-	**1(1)**
대칭/해시	-(2)	-	**-(2)**
기타	-	-(1)	**-(1)**
총합	**3(3)**	**4(5)**	**7(8)**

이후, 2021년 6월 세 번째 PQC 표준화 컨퍼런스가 개최되었고, 3 라운드로 넘어가는 과정에 관한 내용과 각 암호 알고리즘들의 변경점, 그리고 다양한 응용법 및 최적화 방법 그리고 부채널 공격을 포함한 다수의 공격법이 소개되었다[8]. 추가로 3 라운드에서는 표준화 컨퍼런스 뿐 아니라 'Round 3 Seminars' 라는 발표들이 간헐적으로 있을 때마다 중요한 이슈들을 소개하는 자리가 온라인으로 이루어졌다[9].

Ⅴ. 표준 암호 선정과 4 라운드

2022년 7월에 드디어 표준 암호로 격자 기반의 어려움을 기반으로 하는 CRYSTALS-KYBER가 KEM/ENC의 표준으로, CRYSTALS-DILITHIUM과 FALCON 그리고 대칭/해시의 어려움을 기반으로 하는 SPHINCS+가 전자 서명의 표준으로 지정되었다[10]. 전자 서명으로 3개의 알고리즘이 지정된 것에 반해 KEM/ENC 부문에서는 단일 알고리즘만이 선정되었기 때문에 NIST에서는 추가로 4 라운드를 진행하여 현재 코드 기반의 Classic McEliece, BIKE, HQC, 그리고 아이소제니 기반의 SIKE가 후보로 등록되었다[11]. 이후 일정으로는 2022년 12월에 진행되는 네 번째 PQC 표준화 컨퍼런스가 있으며, 당일에 4 라운드에 대한 자세한 내용과 해당 라운드에서 가장 주요하게 생각하는 이슈를 확인할 수 있을 것으로 보인다[12].

Ⅵ. 결론

본 논문에서는 현재 진행 중인 NIST PQC 공모전에 대한 동향을 소개하였으며, 다양한 암호 알고리즘들의 후보로부터 1개의 KEM/ENC과 3개의 전자 서명이 표준으로 선정되었고, 지금도 추가 암호 알고리즘들을 등록받으며 4 라운드를 진행하고 있음을 소개하였다. 양자 컴퓨터 기술과 양자 내성 암호는 앞으로도 큰 이슈이며 쉽게 해결되지 않을 문제이기 때문에 지속적인 관심과 연구에 대한 노력이 필요할 것으로 보인다.

참 고 문 헌

[1] Shor, P. W. "Algorithms for quantum computation: discrete logarithms and factoring", In proceedings 35th annual symposium on foundations of computer science, pp. 124-134.

[2] NIST, "Report on Post-Quantum Cryptography", NISTIR 8105, 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[3] NIST, "Round 1 Submissions", 2017, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Round-1-Submissions.

[4] NIST, "First PQC Standardization Conference", 2018, https://csrc.nist.gov/Events/2018/first-pqc-standardization-conference.

[5] NIST, "Round 2 Submissions", 2019, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions.

[6] NIST, "Second PQC Standardization Conference", 2019, https://csrc.nist.gov/Events/2019/second-pqc-standardization-conference.

[7] NIST, "Round 3 Submissions", 2020, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[8] NIST, "Third PQC Standardization Conference", 2021, https://csrc.nist.gov/Events/2021/third-pqc-standardization-conference.

[9] NIST, "Round 3 Seminars", 2021, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-qua

ntum-cryptography-standardization/round-3-submissions/round-3-seminars.

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

[11] NIST, "Round 4 Submissions", 2022, https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions.

[12] NIST, "Fourth PQC Standardization Conference", 2022, https://csrc.nist.gov/Events/2022/fourth-pqc-standardization-conference.