부호 기반 양자 내성 암호 NIST 표준화 동향

최승주* 권혁동* 서화정*†

*한성대학교 IT융합과

Post Quantum Algorithm and Standardization trend of NIST

Seung-Ju Choi* Hyeok-Dong Kwon* Hwa-Jeong Seo*†

*Division of IT Convergence Engineering, Hansung University.

요 약

최근 양자 컴퓨터 시대에 대비한 양자 내성 암호에 대한 많은 연구가 진행되고 있다. 이러한 움직임에 맞춰 미국 국립표준기술 연구소에서는 2016년 10월 20일부터 양자 내성 암호에 대한 표준화 사업을 진행하였고, 이미 표준화 1라운드는 완료가 되었으며, 2019년 1월 30일부터 표준화 2라운드가 진행되고 있다. 본 논문에서는 양자 컴퓨터와 부호 기반의 양자 내성 암호 중심으로 NIST 표준화 연구의 최신 동향을 살펴본다.

I. 서론

최근 양자 컴퓨터의 활발한 개발과 더불어 양자 내성 암호(Post-Quantum Cryptography)에 대한 많은 연구가 이루어지고 있다. 미국 국립 표준 기술 연구소(National Institute of Standards and Technology, 이하 NIST)에서는 2016년 양자 내성 암호 표준 계획안을 발표하였고 2017년 12월 세계 여러 각국에서 제출한 양자 내성 암호 표준 후보를 선출하였다. 이후 2년간의 평가 기간을 거쳐 2019년 라운드2의 후보로 총 26개의 후보가 발표되었다. 이런 평가 기간 동안 표준 공모전에 제안된 기법들에 소프트웨어 최적화, 안전성 분석 등 여러 가지 관점에서 연구가 이루어졌으며, 다음 라운드의 후보자를 선출하기 위한 연구가 지금도 활발히 이루어지고 있다. 본 논문에서는 양자 컴퓨터와 미국 NIST 양자 내성 암호 표준 연구 동향을 살펴보고자 한다.

II. 양자 컴퓨터와 큐비트

양자 컴퓨터 개념의 등장은 1980년대 초반 R. Feynman이 컴퓨터에 양자 물리학을 적용하자는 아이디어를 제안하면서 등장하였다[1]. 이러한 아이디어가 나오게 된 배경은 양자 물리학의 중첩 상태를 기존의 디지털 컴퓨터로 계산하는 데 있어서 기술적인 한계에 봉착했기 때문이다. 이러한 아이디어가 나온 당시에는 사람들의 큰 관심을 끌지는 못하였지만 1990년대 소인수 분해 양자 알고리즘이 제안되면서 이를 구현하려는 많은 연구가 진행되었다.

기존 컴퓨터와 양자 컴퓨터의 가장 큰 차이점은 컴퓨터 연산을 진행하는 단위의 개념이 달라졌다는 것이다. 기존 컴퓨터는 0과 1중 하나로 비트의 단위로 연산을 하였다면 양자 컴퓨터는 큐비트라는 새로운 단위를 사용한다. 이러한 큐비트는 0과 1이라는 상태를 동시에 가질 수 있으며 이러한 상태를 중첩이라고 부른

다. 이러한 성질을 갖고 있는 큐비트의 상태로 인해 표현할 수 있는 정보의 수가 늘어났고 다량의 큐비트를 활용하면 기하급수적인 정보의 양을 표현할 수 있게 되었다. 또한 큐비트는 얽힘이라는 상태를 가질 수 있는데, 이는 하나의 큐비트의 상태를 측정하였을 때 해당 큐비트와 얽혀있는 다른 큐비트의 상태들이 전부 결정되는 성질이다.

이러한 성질들을 통해 기존 컴퓨터로는 몇백 년이 걸려야 하는 연산을 병렬 연산을 통해 단 몇 분 안에 처리할 수 있게 되었다. 대표적인 연산으로는 소인수분해의 주기성을 찾는 문제로써 수학자 Shor가 제안한 Shor 알고리즘을 [2] 들 수 있다. 해당 알고리즘은 푸리에 변환을 활용하여 한 번의 연산만으로도 소인수 분해에 필요한 지수 계산의 주기를 알아낼 수 있게 하는 양자 알고리즘이다.

비록 해당 알고리즘을 구동할 수 있는 양자 컴퓨터는 아직 개발되지 않았지만, 양자 컴퓨터가 보급이 예상되는 약 10년 뒤의 세상에는 소인수분해 문제를 바탕으로 한 공개키 암호화 알고리즘은 무용지물이 되고 만다. 이러한 양자 컴퓨터를 개발하기 위해 세계적인 기업들이 노력중이다. 마이크로 소프트에서는 양자 컴퓨터용 프로그래밍 언어 Q#을 출시하였으며, 구글은 72큐비트 양자 컴퓨터 브리슬콘을 공개하였고 IBM은 20큐비트 프로세서를 탑재한 양자 컴퓨터 Q System One을 올해 초에 선보였다. 그러나 논리적인 큐비트를 표현하기 위해서는 전자 단위의 물질을 이용해야 하는데 이는 외부 환경의 변화에 매우 취약하다. 이를 해결하기 위해 현재 수많은 기업들은 큐비트의 수를 늘리는 것뿐만 아니라 양자 프로세서의 오류율을 감소시키는 데에도 힘쓰며 양자 컴퓨터 시대의 도래에 힘쓰고 있다.

III. 양자 내성 암호

앞에서 언급한 것처럼 양자 컴퓨터는 기존 컴퓨터로 연산할 수 없었던 많은 문제를 빠르고 쉽게 해결할 수 있을 것이다. 그러나 이러한 연산은 특정 연산에만 적용이 될 뿐 실제로 단순 계산이나 비디오 스트리밍처럼 한 번에 하나의 비트를 처리하는 연산들에 대해서는 오히려 연산 속도가 큰 차이가 없기 때문에 해당 연산을 위해 사용하는 큐비트의 효율성이 떨어지게 된다. 하여 양자 컴퓨터에 적합한 알고리즘들이 연구 되고 있으며 양자 내성 암호 알고리즘 또한 이러한 속성에 맞게 연구 되고 있다.

양자 내성 암호는 격자 기반 암호, 부호 기반 암호, 다변수 다항식 기반 암호, 타원 곡선 기반 암호인 아이소제니 그리고 해시 기반 암호 등으로 수학적 기반 문제에 따라 5가지로 나눌 수 있다. 이러한 암호들은 기존의 비트 기반 컴퓨터의 암호 공격에도 안전성이 검증된 암호들이다. 그러나 현재 많이 사용되고 있는 RSA나 AES 등과 같은 암호 기법들에 비해 느린 연산 속도, 큰 키의 크기 등 효율성이 떨어져 그간 세상의 주목을 받지 못하였다. 그러나 양자 컴퓨터가 점점 발전하게 되면서 양자 컴퓨터를 사용한 공격으로부터 안전한 암호 알고리즘이 필요하게 되었고 이에 양자 내성 암호가 관심을 받게 되었다. 이러한 기존 양자 내성 암호들의 또 다른 특징으로는 오랫동안 많은 공격을 방어해 냈다는 점이다. 비록 효율적이지 못하다는 이유에 의해 사용되지 않았지만 오랜 기간 여러 가지 공격을 방어해 내며 안전성을 보여왔다. 물론 이러한 특성들을 갖고 있다 하더라도 실제로 양자 컴퓨터가 상용화되어 새로운 양자 알고리즘으로 현재 제안되는 양자 암호 알고리즘을 공격하였을 때에도 안전할 것이라는 보장을 할 수 없다. 그렇기에 양자 내성 암호에 대한 검증과 효율성에 대한 연구는 계속 되어야 할 것이다.

IV. NIST 양자내성암호 공모전

2016년 초 미국 국립표준기술연구소 NIST는 양자 컴퓨터의 도래가 기존의 많은 암호 알고리즘의 안전성을 위협할 것이라는 초안을 발표하였다[2]. 같은 달 NIST는 양자 내성 암호 표준화 공모전과 로드맵 <표1>을 발표하고 세계

각국의 암호 연구 기관으로부터 양자 내성 암호 표준 후보를 모집하였다. 공모전에는 한국을 포함한 다양한 기관이 참여를 하였고 Round 1에서는 NIST에서 제시한 공개키 양자 내성 암호 알고리즘과 전자 서명 알고리즘 종합 64개가 선정되었다. 선정된 알고리즘은 부호 기반이 19개, 격자 기반이 26개로 부호 기반과 격자 기반이 주를 이루었으며, 이외에도 다변수 다항식 9개, 해시 기반 3개 외에도 기타 3개로 다양한 유형의 알고리즘이 제출되었다.

<표1> NIST 양자 내성 암호 공모전 로드맵

일정	내용
2016.02	NIST 양자 내성 암호 공모전 발표
2016.10	양자 내성 암호 후보군 요청
2017.12	Round 1 양자 내성 암호 후보 발표
2018.04	1차 양자 내성 암호 표준화 컨퍼런스 개최
2019.01	Round 2 양자 내성 암호 후보 발표
2019.08	2차 양자 내성 암호 표준화 컨퍼런스 개최
2020/2021	Round 3 양자 내성 암호 후보 선정 진행
2022/2024	양자 내성 암호 표준화 완성

Round 2는 로드맵에서 계획했던 것보다 더 빠르게 진행이 되었는데 이는 양자 컴퓨터가 예측했던 것보다 더 빠르게 개발이 될 것이라는 연구 결과를 반영한 것으로 보인다.[3] Round 2는 2019년 1월 30일에 발표가 되었으며 총 26개의 알고리즘이 선정되었다. 선정된 암호 알고리즘 후보의 종류로는 공개키 암호 알고리즘이 17개, 서명 알고리즘이 9개로 구성되어 있다<표2>. Round 2에서 선정된 알고리즘의 주를 이루는 기반 알고리즘 유형은 Round 1 때와 마찬가지로 격자 기반 방식과 부호 기반 방식의 수가 가장 많았다. Round 2에는 최적화와 몇몇 제출된 알고리즘들에 존재하는 결함들에 대한 보완을 요구하였다. 여기에서 최적화는 소프트웨어적 최적화뿐만 아니라 하드웨어에 대한 최적화도 포함이 된다.

Round 2에 선출된 알고리즘들은 NIST에서 제시한 수정사항들을 반영하며 Round 3에 선출될 준비를 하고 있다. 이처럼 양자 내성 암호의 개발은 여전히 과도기에 있으며 실생활에 적용이 가능한 암호를 선출해 내기 위한 연구가 계속되는 것을 볼 수 있다.

<표2> NIST 양자 내성 암호 Round 2

기반	공개키 암호/키 생성	서명
부호	Bike	
	Classic McEliece	
	HQC	
	LEDAcrypt	
	NTS-KEM	
	ROLLO	
	RQC	
격자	CRYSTALS-KHYBER	CRYSTALS-DILITHIUM
	Frondose	FALCON
	LAC	qTESLA
	Newcome	
	NTRU	
	NTRU Prime	
	Round 5	
	SABER	
	Three Bears	
다변수 다항식		GeMSS
		LUOV
		MQDSS
		Rainbow
아이소제니	SIKE	
해시		SPHINCS+
제로 지식 증명		Picnic

4.1 Classic McEliece

Round 2에는 다양한 공개키 알고리즘이 선발되었는데 그 중 McEliece가 가장 대표적인 알고리즘이다. McEliece는 많은 공개키 양자 내성 알고리즘의 근간이 되었으며, 이러한 McEliece 또한 이번 공모전에서 Classic McEliece이라는 이름으로 제출되었다. 부호 기반 알고리즘들의 근간이 되는 해당 알고리즘에 대해 알아보고자 한다.

기존의 McEliece는 1978년 미국 캘리포니아 공과대학교 교수 Robert J.McEliece에 의해 제안된 암호 체계다. 이 알고리즘은 Goppa 부호를 오류 정정 보호로 사용한 공개키 암호 알고리즘으로서 부호 이론을 기반으로 하고 있다. 이 알고리즘은 송신자가 수신자에게 보내는 메시지에 고의로 오류 벡터를 추가하여 오류 수정 부호 없이는 복호화하기 어렵게 만든다. [4]

McEliece는 OW-CPA의 방식을 따라 설계

되었는데 OW-CPA는 부호 코드가 랜덤하게 설정되었을 때 공격자가 공개키와 암호문만으로는 부호 코드를 효과적으로 찾기 어렵다는 뜻이다. 현재는 암호문을 통해 평문을 알아내는 기법을 이용한 공격 방식인 CCA에 대한 보안 체계인 CCA 2-security(adaptive chosen-ciphertext attack) 또한 보장한다. 또한 캡슐화와 복호화 과정이 매우 빠르다는 특징을 갖고 있으며. 하드웨어적으로 키 생성이 매우 빠르다. 암호문 사이즈는 다른 현재 사용되고 있는 암호 알고리즘의 암호문에 비해 크기가 크지만 제안되고 있는 다른 양자 내성 암호와 비교했을 때는 작다.

이렇게 만들어진 McEliece 알고리즘은 지난 40년간 수많은 공격에도 암호의 체계가 깨지지 않았을 만큼 안전성이 보장된 암호 체계였으나. 다른 암호들에 비해 키의 크기가 커서 주로 사용되지 않았다. 그러나 양자 컴퓨터의 시대가 가까워짐에 따라 기존 암호 알고리즘의 안전성이 깨질 위협에 처했다. McEliece가 양자 컴퓨터의 연산력에도 안전하다고 판단되어 양자 내성 암호로서 다시 사람들의 주목을 받게 되었다.

V. 결론

양자 컴퓨터 시대가 다가옴에 따라 양자 내성 암호 알고리즘이 필요해진 상황이다. 이에 미국 국립 표준 기술 연구소에서는 양자 내성 암호 공모전을 개최하여 각국에서 양자 내성 암호 후보들을 모아 선출하였다. NIST는 이 공모의 목적은 알고리즘 하나만을 선출하는 것이 아니기 때문에 여러 개의 후보가 양자 내성 암호의 표준이 될 수 있다고 발표하였다.

NIST에서는 암호의 선출을 안전성과 실용성을 기준으로 잡고 있다. 현재 선출된 후보들은 선출 과정에서 제시된 수정 사항들을 지속해서 반영하면서 기준에 맞추기 위해 수정해 나가고 있다. 앞으로 진행되는 NIST의 양자 내성 암호 표준화 사업에 주목해야할 필요가 있다.

[참고문헌]

[1] R. Feynman, Simulating Physics with Computers, International Journal of Theoretical Physics 21, 467, 1982.

[2] Peter W. Shor, Algorithms for Quantum Computation: Discrete Log and Factoring, Proceedings 35th Annual Symposium on Foundations of Computer Science , 1994.

[3] Michele Mosca, Cybersecurity in an era with quantum computers: will we be ready?, 2019.

[4] Jacques Stern, A new identification scheme based on syndrome decoding, 1993.

[5] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone, Report on Post-Quantum Cryptography, NIST IR 8015 DRAFT, 2016.

[6] Classic McEliece Comparison Task Force, Classic McEliece vs NTS-KEM,, June, 2018.

[7] RJ McEliece, A public-key cryptosystem ased on algebraic, 1978

[8] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, Paulo S. L. M. Barreto, MDPC-McEliece: New McEliece Variatns from Moderate Density Parity-Check Codes, 2013

[9] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8240, 2019