제1회 NIST Post-Quantum Cryptography 표준화 회의

유용석 인천대학교 조교수

1. 머리말

양자컴퓨터의 상용화가 가시화되면서 기존의 전통적인 컴퓨터를 가정한 계산 복잡도 기반의 암호화 알고리즘들의 보안성이 근본적으로 위협 받고 있다. 따라서 세계적으로 널리 쓰이고 있는 RSA 알고리즘과 같은 계산 복잡도 기반의 현대 암호 기술을 대체할 Post-Quantum Cryptography 기술이 활발히 연구되고 있다. 최근 미국 표준을 담당하고 있는 NIST에서는 2017년 11월까지 신규 알고리즘을 공모한 후 제출된 기법들에 대한 논의를 하기 위해 2018년 4월 첫 번째 Post-Quantum Cryptography 표준화 회의를 주최하였다.

이번 회의는 2018년 4월 11일부터 13일까지 미국 포트로더데일에서 개최되었고, 25개국에서 제출된 62개의 제안서에 대한 발표가 이루어졌다. 진행 방식은 각 알고리즘을 제안한 단체에서 제안하는 기법에 대해서 15분 동안 발표하고 질문을 받는 형식으로 진행되었다. 본고에서는 이번 표준화 회의의 내용을 분석하여 북미의 Post-Quantum Cryptography 표준화 동향을 파악하고 향후 대응 전략을 도출하고자 한다.

2. 주요 회의 내용

2.1 NIST의 Post-Quantum Cryptography 표준화 전략 및 일정

그동안 Post-Quantum Cryptography의 국제 표준화는 유럽의 ETSI를 중심으로 진행되었으나, 최근 NIST에서 2017년 11월까지 차세대 보안 기술을 공개적으로 모집하고, 2018년 4월, 제1회 공식 표준화 회의를 주최하는 등 적극적인 움직임을 보이고 있다.

NIST가 제시한 표준화 일정은 〈표 1〉과 같다.

<표 1> NIST의 Post-Quantum Cryptography 표준화 일정

일 정	내 용
2015년 4월 11-13일	제 1회 NIST Workshop on Cybersecurity in a Post-Quantum World
2016년 12월 20일	Call for Proposals
2017년 11월 30일	Deadline for submissions
2018년 4월 11-13일	제 1회 Post-Quantum Cryptography 표준화 회의
2019년 8월	제 2회 NIST PQC Workshop
2020~2021년	알고리즘 선정 혹은 3rd Round
2022~2024년	Post-Quantum Cryptography 표준 문서화

<표 2> NIST Post-Quantum Cryptography level

Level	보안성
I	AES128 만큼 해독하기 어려움
II	SHA256 만큼 해독하기 어려움
III	AES192 만큼 해독하기 어려움
IV	SHA384 만큼 해독하기 어려움
V	AES256 만큼 해독하기 어려움

NIST는 2015년 4월 워크숍을 주최한 이후 2016년 12월에 Post-Quantum Cryptography 기술에 대한 제안서를 공지하고, 2017년 11월까지 표준화 기술을 공모받았다. 이번 표준화 회의를 기점으로 Post-Quantum Cryptography에 대한 표준화를 공식적으로 시작하였다. 이번 회의에서는 2017년 11월까지 제안받은 기술들 중 제출 요건을 만족한 64개 기술을 대상으로 62개의 발표를 진행한 후 2019년 8월 경 2차 워크숍을 통해 후보군을 압축하여 (round 2) 발표할 계획이다. 이후 2021년까지 알고리즘 선정을 마치고 2022년부터 약 2년 정도의 기간 동안 표준 기술의 문서화 작업을 진행하여 2024년에 Post-Quantum Cryptography 기술의 표준화를 완료할 계획이다.

2.2 제 1회 공식 표준화 회의 동향

NIST는 〈표 2〉와 같이 5단계의 Post-Quantum Cryptography 기술을 공모하였다. 이 중에서 Level I, III, V는 암호화 기술이며, Level II와 IV는 인증 기술이다.

2017년 11월까지 25개국에서 82개의 Post-Quantum Cryptography 기술 제안서가 NIST에 제출되었다. 그 중에 64개 제안서가 제출 요건을 만족하여 Round 1을 통과하였고, 이번 표준화 회의에는 62개의 제안서가 2박 3일 동안 발표되었다. 각 제안서의 발표 시간은 질문을 포함하여 15분으로 제한되었기 때문에, 기술적으로 심도 깊은 논의 보다는 제안하는 기법의 소개와 특징을 간략히 소개하는 수준으로 진행되었다.

제안된 기법들 중 가장 많은 수인 26개의 기법이 lattice 기반 알고리즘이었다. 이는 Post-Quantum Cryptography를 구현하기 위한 기술로 lattice 기반의 기법이 가장 큰 관심을 받고 있음을 보여준다. Learning with Errors(LWE)와 그 변형인 Ring LWE 그리고 NTRU와 같은 lattice 기반의 보안 기술들은 그 보안성이 이론적으로 증명되었기 때문에 보안성 측면에서는 가장 기대되는 접근 방식이다. 하지만 이를 구현하기 위해서는 기존에 사용되는 것과는 전혀 다른 난수 발생 기법과 장치가 필요하기 때문에 lattice 기반의 기술을 실용화하는 방법이 관건이 될 것이다.

그 다음으로 많은 19개의 제안서는 code 기반 기법이었다. Code 기반의 기법은 전통적으로 정보이론 분야에서 연구되고 활용되는 이론적 도구들로 해석하고 분석할 수 있으며, 실제 구현을 위해서 기존에 널리 활용되는 소프트웨어와 하드웨어를 활용할 수 있기 때문에 실용성 측면에서도 선호되는 접근 방법이다.

다른 접근 방식으로 mutivariate 기반의 Rainbow와 같은 기법도 활발히 제안되고 있으나, 실용적인 구현 방법에는 더 논의가 필요한 것으로 판단된다. 그 이외에도 isogeny 기반의 기법과 hash 기반의 기

법도 활발히 논의되고 있다.

이번에 제안된 기법들에 대한 NIST 내부 검토를 거쳐서 2019년 8월 워크숍에서 round 2 진출 여부가 발표될 예정이다.

3. 맺음말

Post-Quantum Cryptography에 대한 연구 개발이 활발히 진행되고 있는 가운데, NIST도 본격적인 표준화 활동을 시작하였다. 이번 제1회 NIST Post-Quantum Cryptogphy 표준화 회의에서는 25개 국가에서 82개의 제안서를 제출하여 Post-Quantum Cryptography 기술의 표준화에 대한 국제적인 관심을 확인할 수 있었다. 이 기술을 위해 다양한 접근 방법들이 제안되고 있으며, 가장 큰 관심을 받고 있는 기술은 lattice 기반과 code 기반의 암호화 기법이다.

NIST는 2021년 경까지 Post-Quantum Cryptography 표준 기술을 선정할 계획이며, 그 이후 2년여 정도의 문서화 작업을 거쳐 2024년까지 표준화를 완료할 계획이다.

현대 암호기술을 대체할 Post-Quantum Cryptography의 표준화 동향에 대한 면밀한 분석과 이에 대한 선제적인 대응이 무엇보다 중요한 시점이다.

※ 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음 [2015-0-00781, 양자암호통신 분야 QKD 기술 표준개발].

정보통신 용어 사전 http://terms.tta.or.kr

술어 논리 Predicate logic

객체 사이의 관계를 나타내는 논리 또는 형식 체계.

명제 논리의 모든 요소를 포함하고 보다 효율적인 지식 표현이 가능하다. 명제 논리와 마찬가지로 지식 표현 및 추론에 사용된다. 술어 논리에서 객체는 상수나 변수 혹은 함수로, 관계는 술어로 표현된다. 객체의 집합이 가지는 특성은 변수와 한정 기호(quantifier)로 표시된다. 하나의 술어로 구성되는 원자(atomic) 문장은 참 혹은 거짓 중 하나의 값을 가지고, 연산자로 연결되어 복합 문장을 구성한다. 술어 논리는 기호 기반 인공 지능에서 사용하는 지식 표현 및 추론의 모체가 되었다. 그 대표적인 예로 존 로빈슨(John A. Robinson)이 1965년 제안한 해결법(resolution method) 및 이에 기반한 프로그래밍 언어인 프롤로그(PROLOG) 등을 들 수 있다. 프롤로그(PROLOG)는 IBM에서 개발한 인공 지능 기반 질의응답 시스템인 왓슨(Watson)의 자연어 처리에 활용되었다.