NIST PQC 표준화 현황

송민호

유튜브 주소: https://youtu.be/PxZJG9iEdgk

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

양자 내성 암호

- 현대 암호는 수학적 문제에 의존
  - Shor, Grover 알고리즘으로 인한 위협
  - Shor: 인수 분해와 같은 작업을 효율적으로 수행
  - Grover: brute force attack 가속화(대칭키 위협)

- 양자 공격에 저항할 수 있는 새로운 암호 알고리즘
  - 격자 기반, 코드 기반, 해시 기반 등

- NIST PQC 표준화 공모전 진행
  - 효율적인 양자 내성 암호 알고리즘 식별 및 표준화

NIST PQC round 1

- 69개의 양자 내성 암호 알고리즘 선정
  - 철회된 알고리즘 5개 포함

유형	공개 키 암호/키 생성	서명
격자	CRYSTALS-Kyber NTRU SABER FrodoKEM NTRU Prime LAC NewHope Round5 Three Bears Compac LWE Ding Key Exchange DMBLEM and R.EMBLEM HILA5 KCL(pka OKCN/AKCN/CNKE) KINDI LIMA Lizard LOTUS NTRUEncrypt NTRU-HRSS-KEM Odd Manhattan Round2 Titanium	CRYSTALS-DILITHIUM FALCON qTESLA DRS pqNTRUSign
코드	ClassicMcEliece BIKE HQC LEDAcrypt NTS-KEM ROLLO RQC BIG QUAKE DAGS	pqsigRM RaCoSS RankSign
해시		SPHINCS+ Gravity-SPHINCS
다변수다항식	CFPKM	Rainbow GeMSS LUOV MQDSS
아이소제니	SIKE	
제로지식증명		Picnic

NIST PQC round 2

- 2019.01.30. 진행
- 26개의 암호가 후보로 선정
- 알고리즘 제외 이유
  - 공격법 발견, 실용성 등

유형	공개 키 암호/키 생성	서명
격자	CRYSTALS-Kyber NTRU SABER FrodoKEM NTRU Prime LAC NewHope Round5 Three Bears	CRYSTALS-DILITHIUM FALCON qTESLA

유형	공개 키 암호/키 생성	서명
코드	ClassicMcEliece BIKE HQC LEDAcrypt NTS-KEM ROLLO RQC	
해시		SPHINCS+
다변수다항식		Rainbow GeMSS LUOV MQDSS
아이소제니	SIKE	
제로지식증명		Picnic

NIST PQC round 3

- Finalists 7개
- Alternate 8개

유형	공개 키 암호/키 생성	서명
격자	CRYSTALS-Kyber NTRU SABER	CRYSTALS-Dilithium FALCON
코드	ClassicMcEliece	
다변수다항식		Rainbow

Finalists

유형	공개 키 암호/키 생성	서명
격자	FrodoKEM NTRU Prime	
코드	BIKE HQC	
해시		SPHINCS+
다변수다항식		GeMSS
아이소제니	SIKE	
제로지식증명		Picnic

Alternate candidates

NIST PQC round 3

- 2022.07.05. 표준 암호 최종 선정
- KEM 방식: CRYSTALS-KYBER
- 서명 방식: CRYSTALS-Dilithium, FALCON, SPHINCS+

유형	공개 키 암호/키 생성	서명
격자	CRYSTALS-Kyber	CRYSTALS-Dilithium FALCON
해시		SPHINCS+

Selected Algorithms 2022

NIST PQC round 4

- KEM 방식은 CRYSTALS-KYBER 유일

- SIKE는 공격법 발견으로 인한 제외

유형	공개 키 암호/키 생성
코드	BIKE Classic McEliece HQC
아이소제니	SIKE

선정 기준

- 고전 및 양자 공격이 기준
  - AES, SHA 공격에 필요한 자원

- LEVEL 1, 2, 3은 수십년간 안전할거라고 생각

LEVEL	보안 정도
1	적어도 AES128 깨기 어려운 정도(exhaustive key search)
2	적어도 SHA256 깨기 어려운 정도(collision search)
3	적어도 AES192 깨기 어려운 정도(exhaustive key search)
4	적어도 SHA384 깨기 어려운 정도(collision search)
5	적어도 AES256 깨기 어려운 정도(exhaustive key search)

NIST 선정 보안 기준

선정 기준

- 수행 능력
  - 다양한 고전 플랫폼에서 측정
- 기존 프로토콜 및 네트워크와의 호환성
- 철저한 비밀 유지
- 부채널 공격에 대한 안전성
- 단순성 및 복잡성

CYRSTALS-KYBER

- KYBER-512는 AES-128과 거의 동등한 보안을 목표
- KYBER-768는 AES-192과 거의 동등한 보안을 목표
- KYBER-1024는 AES-256과 거의 동등한 보안을 목표

- KYBER-768, KYBER-1024 표준화 예정
  - 보안강도 3, 4

- KYBER-512도 표준화 계획 있음
  - 보안강도 1

- 90S 버전은 표준화 X

CRYSTALS-Dilithium

- 기본 서명 알고리즘으로 사용하는 것이 좋다고 전달함

- Dilithium에 대한 표준화 계획
  - 보안 강도 2, 3, 5

- AES 변형 모델은 고려하지 않음(Dilithium-AES)
  - Round 2에 대해 업데이트한 변형 모델
  - SHAKE 대신 카운터 모드에서 AES-256을 사용한 버전

FALCON

- FALCON에 대한 표준화 계획
  - 보안 강도 1, 5
- Dilithium에 비해 크기가 작음
  - 비용이 저렴함
- Dilithium 이후 표준화 예정

SPHINCS+

- SPHINCS+에 대한 계획
  - 보안 강도 1, 3, 5
  - 허용 해시 함수: SHAKE, SHA2
  - SHA2는 보안 강도 1
  - SHA256 & SHA512 MIX 보안 강도 3, 5

- SIMPLE Verison 표준화 예정(ROBUST Version X)
  - Robust version: Round 1에 제출한 버전
  - Robust verison에 비해 속도가 3배 빠름

- FAST, SMALL Version 포함

Q & A