Post-quantum 으로의 마이그레이션 조사

송경주, 장경배, 김현지, 양유진, 임세진, 서화정

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

서론

- 정보화 시대에서 데이터들이 클라우드 및 데이터 베이스 등 전자적으로 저장되어 관리된다 → 인터넷, 모바일, IoT 등 모든 분야에 널리 사용 되고 있는 암호의 중요성 증가
- 양자 컴퓨터는 빠르게 개발되고 있는 분야이며 대형 양자 컴퓨터가 개발되면 현재 사용하는 암호들이 양자 알고리즘에 의해 더이상 안전하지 않다는 것이 널리 알려져 있다
  - **Grover's algorithm** : 정렬 되지 않은 데이터 베이스에서 특정 데이터를 찾는 속도를 높여 대칭키 암호에 위협이 됨
  - **Shor's algorithm** : 다항 시간 안에 인수분해를 수행하여 공개키 암호에 위협이 됨

- 양자 후 시대에서 암호에 대한 위협을 방지하기 위해 National Institute of Standards and Technology (NIST)에서는 양자 내성 암호(PQC)를 표준화 하기 위한 작업을 진행하고 있다

본 논문에서는 양자 내성 암호(PQC)와 quantum-safe cryptography(QSC)의 마이그레이션을 위한 과정 및 사례를 조사하였다

Post-quantum cryptography(PQC)

- NIST에서는 안전한 PQC 표준을 정하는 것을 목표로 총 3라운드의 post quantum conference을 진행하였다.

- PQC의 후보로는 크게 격자 기반, 코드 기반, 해시 기반, 다변수 기반, 아이소제니 기반이 있으며 후보 암호는 각 quantum-safe한 문제로 안전성을 보장한다.
  - **격자 기반 암호** : NP-hard 기반의 안전성을 가지며 다양한 응용 환경이 지원되고 구현 속도가 빠르고 변수 설정이 어려움.
  - **코드 기반 암호** : 알려지지 않은 오류 수정 코드를 디코딩 하는 문제를 기반으로 안전성을 가지며 암복호화가 빠르지만 키 사이즈가 큼
  - **다변수 기반 암호** : 많은 변수로 이루어진 함수 식을 계산하는 것이 어렵다는 문제에 기반하며 서명 크기가 작고 계산 속도가 빠르지만 키 사이즈가 큼
  - **아이소제니 기반 암호** : 타원 곡선의 아이소제니 연산 문제를 기반으로 하며 구현이 편리하고 키 사이즈가 작지만 연산 속도가 느림
  - **해시 기반 암호** : 해시 함수의 collision resistance 문제에 기반하며 안전성 증명이 가능하고 키 사이즈가 큼

Post-quantum cryptography(PQC)

- 2020년 7월 22일 NIST는 <표 1>, <표 2>와 같이 7개의 finalist와 8개의 alternate를 발표하였다.

<표 1> NIST 에서 발표한 PQC finalist 알고리즘

알고리즘	기반 문제	기능
Rainbow	다변수	전자서명
Classic McEliece	코드	PKE/KEM
NTRU	격자	
CRYSTALS-KYBER		
SABER		
CRYSTALS-DILITHIUM		전자서명
FALCON		

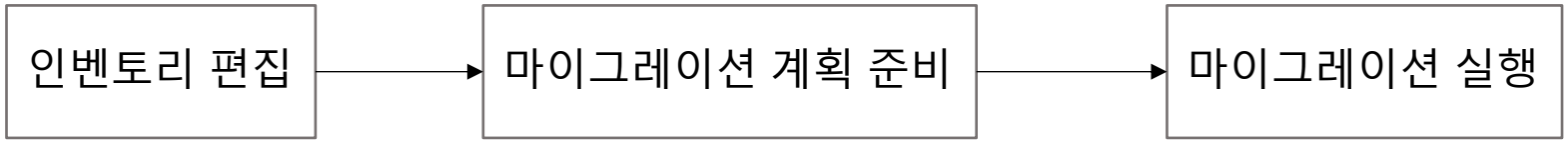
<표 2> NIST 에서 발표한 PQC alternate 알고리즘

알고리즘	기반 문제	기능
FrodoKEM	격자	PKE/KEM
NTRU-Prime		
SIKE	아이소제니	
HQC	코드	
BIKE		
GeMMS	다변수	전자서명
SPHINCS+	해시	
Picnic	영지식증명	

Quantum-safe cryptography(QSC) 마이그레이션 과정

- QSC 마이그레이션 전환 단계

- Non-QSC에서 QSC로 전환하는데 필요한 과정은 다음과 같이 3단계로 진행된다



<3단계 마이그레이션 plan>

인벤토리(시스템) 편집 : 시스템에서 암호화 자산 및 프로세스를 식별하고 마이그레이션 대상이 암호화 하는 엔티티 및 기능을 식별

마이그레이션 계획 준비 : 자산의 전체 목록과 자산에 대한 정보를 기록함. 이때, 공개키 및 대칭키 암호로 암호화된 자산은 각각 마이그레이션 이후에도 동일한 방식으로 암호화 됨. 마이그레이션 과정에서 quantum-safe암호는 더 큰 공개키 및 서명을 포함하므로 PKI의 기능이 QSC를 처리할 수 없는 경우 교체해야 하며 QSC로 업그레이드 된 PKI에는 quantum-safe 서명이 포함된 새로운 인증서가 필요함.

(추후 quantum-safe알고리즘의 취약점이 발견되면 다른 quantum-safe알고리즘으로 수정 및 전환하여 취약점을 해결 해야 함)

마이그레이션 실행 : 인벤토리 편집, 마이그레이션 계획 작성에서 계획한 것을 구현하는 단계, 계획의 실행 가능성을 결정하기 위해 마이그레이션을 시뮬레이션 하고 테스트를 수행함

Quantum-safe cryptography(QSC) 마이그레이션 과정

- 양자 내성 암호 전환 과정 및 고려사항

United States Department of Homeland Security (DHS)은 NIST와의 파트너십을 통해 양자 내성 암호 전환을 위해 조직이 취해야 하는 조치에 대한 로드맵을 만들었다. 로드맵은 다음과 같이 7단계로 진행된다.

1) 표준 개발 조직과의 협력
2) 중요 데이터 목록화
3) 암호화 기술 목록화
4) 내부 표준 식별
5) 공개키 암호 식별
6) 교체 시스템 우선 순위 지정
7) 전환계획

Quantum-safe cryptography(QSC) 적용 방안

1. Network security protocols

두 대상이 네트워크를 통해 안전하고 인증된 통신 링크를 설정하려고 할 때, 한쪽 혹은 양쪽은 통신하고자 하는 상대방의 Public Key Infrastructure(PKI)에서 서명된 인증서를 얻는 방식을 사용한다.

1.1 Transport Layer Security (TLS) cryptography

- TLS는 컴퓨터 네트워크를 통해 통신 보안을 제공하는 암호화 프로토콜로서 웹 클라이언트와 서버 간에 교환되는 데이터를 보호한다.
- 양자컴퓨터가 발전함에 따라 추후 현재 사용하고 있는 TLS통신 알고리즘이 깨질 위험이 있다.
- TLS는 키 설정 및 인증 서비스를 위해 PKI가 지원하는 공개키 암호를 광범위하게 사용하며 이를 quantum-safe하게 업데이트 하는 것이 필요하다.
- TLS는 공개키 암호 뿐만 아니라 대칭키 암호도 사용하는데(데이터 암호화: AES, 디지털 서명 및 인증서 확인: SHA), 대칭키 암호는 block 크기 및 key 길이를 늘려 quantum-safe로 쉽게 바꿀 수 있으므로 공개키에 초점을 맞추고 있다.

Quantum-safe cryptography(QSC) 적용 방안

- TLS에 양자 내성을 적용한 방법으로는 Drop-in replacement, Hybrid scheme, Re-engineering 등이 있다.

  - **Drop-in replacement** : 가장 간단한 제안으로, 현재 공개키 일부 또는 전체를 유사한 quantum-safe drop-in replacement로 교체하는 방식
  - **Hybrid scheme** : 신뢰할 수 있는 기존 key agreement scheme(키 합의 방식)와 새로운 quantum-safe agreement scheme의 출력에서 암호화 키를 파생시키는 hybrid 방식이다. 이 방식은 quantum-safe 암호 변경의 중간 단계로 볼 수 있으며 추가 기능 및 보안을 제공
  - **Re-engineering** : 인터넷 인프라를 재설계하고 시스템 엔지니어링 접근 방식을 사용하여 성능 문제를 완화하고 더 큰 key 크기를 처리할 수 있도록 하는 방식

Quantum-safe cryptography(QSC) 적용 방안

2. Authentication (인증)

- Internet-based application 인증에서는 많이 사용되는 ECDSA 및 RSA 서명을 quantum safe drop-in replacement 하는 방법이 있으며 오프라인 파일 인증에서는 중요한 정보가 포함된 파일을 오랜 기간 동안 원본으로 유지해야 하므로 이 경우에도 ECDSA 및 RSA 서명을 quantum safe drop in replacement로 전환하는 방법이 적합하다.
- 오프라인은 온라인 보다 속도 및 대역폭이 비교적 자유롭기 때문에 hash-tree 서명이 잠재적인 대안으로 제안된다.

결론

- 과거 추상적인 개념이던 양자컴퓨터가 빠르게 개발되며 향후 대규모 양자컴퓨터 개발 시 현재 사용하는 암호에 대해 위협이 될 것이라 예측한다.
- 양자컴퓨터 공격에 대비하기 위해 NIST는 PQC 표준을 정하기 위해 post quantum conference을 개최하였으며 QSC 마이그레이션에 대한 연구가 진행되고 있다.
- 본 논문에서는 양자 후 시대에 대비하기 위해 NIST의 PQC post quantum conference에서 발표한 PQC 후보와 QSC 마이그레이션 과정 및 적용 방안에 대해 조사하였다.

Q & A