국내외 양자내성암호 적용 동향 분석

CryptoCraft Lab

한성대학교 양유진, 장경배, 임세진, 오유진, 서화정

1. Background

- 양자 역학 기술을 기반으로 개발된 양자컴퓨터와 양자 알고리즘(Grover, Shor)의 등장은 암호체계를 위협하는 수단이 될 수 있음
  → 보안적 위협에 대처하기 위해 양자내성암호(Post-Quantum Cryptography) 등장
- 양자컴퓨터를 이용한 공격에 내성을 갖는 양자내성암호는 알고리즘이 기반으로 하고있는 수학적 난제에 따라 5가지(격자, 코드, 해시, 아이소제니, 다변수 기반)로 분류함
- 양자내성암호 표준화 작업이 진행됨에 따라 국내외 기업에서 양자내성암호의 전환을 위해 해당 암호를 적용하는 사례 증가하고 있음

국내외 기업에서 양자내성암호를 적용한 사례를 살펴보며 공통적인 특징과 각 사례들이 갖는 고유한 특징을 분석함

2. 양자내성암호 표준화 동향

국외

- 16년, 미국의 NIST에서 양자내성암호 표준화 공모전 개최
- 22년 7월, 표준화 알고리즘 4개(격자3, 해시1)를 채택
  - 격자기반 암호로의 집중되는 문제를 해소하기 위해 대체 알고리즘 4개 추가 선정
  - 22년 8월, 아이소제니기반 암호인 SIKE의 보안 결함이 밝혀졌음

PQC Primitive	Algorithm	Type	Status
Digital Signature	SPHINCS+	Hash	Standard
	Dilithium	Lattice	
	FALCON		
KEM/PKE	Kyber		
	BIKE	Code	Alternative (Round 4)
	Classic McEliece		
	HQC		
	SIKE	Isogeny	Broken

[표1] NIST 양자내성암호 표준화 공모전 결과

- 22년 7월, 전자서명 알고리즘 공모전 시작 (진행중)
- 23년 8월, 1라운드 진출자로 40개의 알고리즘이 공개됨

국내

- 22년 양자내성암호연구단에서 KpqC 공모전 개최 (진행중)
- 16개의 알고리즘이 1라운드 알고리즘으로 채택

PQC Primitive	Algorithm	Type
Digital Signature	GCKSign, HAETAE, Peregrine, SOLMAE	Lattice
	Enhanced pqsigRM	Code
	AIMer	Other
	FIBS	Isogeny
	MQ-Sign	Multivariate
KEM/PKE	NTRU+, SMAUG, TiGER	Lattice
	Layered ROLLO-I, REDOG, PALOMA	Code
	IPCC	Other

[표2] KpqC 공모전 1라운드 알고리즘

- 23년 12월, 1라운드 결과가 발표될 예정
- 24년, 2라운드를 진행하여 최종 알고리즘을 선정할 계획
- 3라운드 진행 여부는 검토하고 있음
  - 선정된 알고리즘을 실제 현장에 적용할 때 고려되는 사항을 논의하기 위함

3. 양자내성암호 적용 동향

국외

1. 구글

- CECPQ1 (Combined elliptic-curve and post-quantum 1)
  - 구글이 개발한 양자 내성 키 합의 프로토콜
  - Round 2 후보였던 NewHope(격자기반)와 X25519(타원곡선)를 결합한 프로토콜
  - 16년, 테스트용 브라우저 " 크롬 카나리아 " 의 TLS에 적용
- CECPQ2
  - X25519와 NTRUHRSS(격자기반) 결합
  - CECPQ2b는 NTRUHRSS 대신 SIKE(아이소제니기반) 적용
  - 호환성 문제로 23년 4월 크롬 지원 중단
- X25519Kyber768
  - X25519와 표준화 알고리즘으로 선정된 Kyber768(격자기반) 결합
  - 23년 8월, " 크롬 버전 116"에서 제공

2. IBM

- Key Protect (암호화 키 관리 서비스)에 요청 보낼 때 사용되는 TLS 연결 과정의 키를 보호할 때 사용됨
  - Hybrid mode
    - ECDH와 Kyber를 결합한 모드
    - 키 크기별로 3가지 매개변수 제공 (p256_kyber512 / p384_kyber768 / p521_kyber1024)
  - Quantum safe mode
    - Kyber를 온전히 제공하는 모드
    - 키 크기별로 3가지 매개변수 제공 (kyber512 / kyber768 / kyber1024)
- 유일하게 하이브리드가 아닌 양자내성암호만 적용한 TLS 제공
- 그러나, 리눅스에서만 해당 기술을 사용할 수 있음

3. AWS

- s2n-tls
  - 기존의 타원곡선 암호에 양자내성암호를 적용한 프로토콜
  - 공모전 진행 중에는 CRYSTALS-Kyber, SIKE, BIKE를 제공하였으나 결과가 나온 후에는 최종 선정 알고리즘인 Kyber만 제공

[적용가능한 서비스]
- KMS(암호화 키 생성 및 제어)
- ACM(SSL/TLS 인증서 관리)
- AWS Secret Manager(DB 자격 증명, API 키 관리, 기타 보안 암호 관리)

국내

1. LG U+

- 국내에서 양자내성암호 개발 및 적용에 유리한 고지를 선점하고 있다 평가됨
- 20년 6월, 코위버의 광전송장비(ROADM)에 양자내성암호 기술 탑재에 성공
- 22년 4월, 세계 최초로 PQC 전용회선 서비스(PQC 전송장비) 출시
- 22년 9월, 국내 최초로 eSIM에 물리적 복제 방지기능(PUF)와 양자내성암호를 탑재 (PQC PUF-eSIM)
- U+ 지능형 CCTV에 암호화된 VPN을 구현하는 통신 프로토콜(와이어가드)에 양자내성암호를 결합한 기술 적용
- 서울대 Cryptolab에서 개발한 양자내성암호 Rlizard를 사용함
  - NIST 표준화 공모전 2라운드에서 보안강도 검증된 격자기반 알고리즘
  - KpqC 표준화가 완료되면 선정된 알고리즘으로 교체할 계획이라 명시함

2. 우리넷

- 23년 7월, 패킷광전송장비(POTN)에 CRYSTALS-Kyber를 적용해 상용화 성공
- 보안 전송 서비스의 확대를 기대하고 있음

4. Analysis

- 국외의 경우 대부분 TLS에 사용되는 타원곡선 암호의 전환에 사용됨
- 세 기업 모두 CRYSTALS-Kyber를 사용
- 대부분의 기업이 호환을 위해 하이브리드 형태로 제공
- 국내에서는 LG U+를 비롯한 기업에서 TLS 외의 다양한 분야에 양자내성암호를 적용함

	기업명	알고리즘	적용 내용
국외	Google	CRYSTALS-Kyber + ECDH (Hybrid)	(X25519Kyber768) Chrome version 116
	AWS		(s2n-tls) KMS, ACM, AWS Secret Manager
	IBM		IBM Cloud - Hybrid mode
		CRYSTALS-Kyber	IBM Cloud - Quantum safe mode
국내	우리넷		패킷광전송장비
	LG U+	Rlizard	PQC 전송장비, PQC PUF-eSIM, PQC VPN 등

[표3] 최근 국내외 양자내성암호 적용 사례

5. Conclusion

국외

- IQT Research는 3번째 PQC 분석 보고서에서 2032년까지 PQC 수익이 67억 달러(한화 8조 9천억원)까지 증가할 것이라 예측
- 양자내성암호에 대한 중요성이 커짐에 따라 기업에서 양자내성암호를 적용하는 사례가 증가할 것으로 예상됨

국내

- 23년 7월, 정부가 발표한 양자내성암호 전환을 위한 마스터플랜에 따르면, 2035년까지 국내 암호체계들을 양자내성암호로 전환하는 것을 목표로 두고 있음
- 국내에서도 양자내성암호의 중요성이 커지며 기업에서 이를 적용하는 사례가 증가할 것이라 기대됨