국내외 양자내성암호 적용 동향 분석

양유진*, 장경배*, 임세진*, 오유진*, 서화정**

*한성대학교 (대학원생)

**한성대학교 (교수)

Analysis of Trends Applying Domestic and Foreign Post-Quantum Cryptography

Yu-jin Yang*, Kyung-bae Jang*, Se-jin Lim*,

Yu-jin Oh*, Hwa-jeong Seo**

*Hansung University (Graduate student)

**Hansung University (Professor)

요 약

기존 컴퓨터보다 특정 문제를 빠르게 해결할 수 있다 알려진 양자 컴퓨터의 개발은 현존하는 암호체계의 위협이 될 것으로 예상된다. 이를 대비하기 위해 양자내성암호가 등장하였고 국외에서는 NIST에 의해, 국내에서는 양자내성암호연구단에 의해 표준화 작업이 진행되고 있다. 표준화 작업의 진행에 맞춰 기업에서는 양자내성암호로의 전환을 위해 해당 암호들을 적용하고 있다. 본 논문에서는 국내외 기업에서 양자내성암호를 적용한 사례들을 살펴보며 분석한다.

I. 서론

양자 중첩 및 얽힘과 같은 양자 역학 기술을 기반으로 개발된 양자 컴퓨터는 특정 문제를 기존 컴퓨터보다 빠르게 해결할 수 있다는 특징을 갖는다. 그러나 이 특징은 Grover, Shor와 같은 양자 알고리즘과 함께 사용될 경우 암호 체계를 위협하는 수단이 되기도 한다. 양자 컴퓨터 및 양자 알고리즘에 의한 보안적 위협에 대비하기 위해 양자 컴퓨터를 이용한 공격에 내성을 갖는다는 의미를 가진 양자내성암호(Post-Quantum Cryptography, PQC)가 등장하였다. 일반적으로 양자내성암호는 암호 알고리즘이 기반으로 하고 있는 수학적 난제에 따라 총 5가지(격자, 코드, 해시, 아이소제니, 다변수 기반)로 분류되며 이 중 격자, 코드기반의 암호가 NIST에서 주최한 양자내성암호 표준화 공모전에서 주목을 받았다. 표준화 작업이 진행됨에 따라 국내외 기업에서 양자내성암호로의 전환을 위해 해당 암호를 적용하고 있는 상황이다. 이에 본 논문에서는 국내외 기업에서 양자내성암호를 적용한 사례들을 살펴보며 공통적인 특징과 각 사례들이 갖는 고유한 특징에 대해 분석한다.

II. 양자내성암호 표준화 동향

본 장에서는 양자내성암호를 적용한 사례들을 살펴보기에 앞서 기업들이 적용한 양자내성암호에 대한 이해를 돕기 위해 표준화 동향에 대해 살펴본다.

2016년, 미국의 NIST는 양자내성암호 표준화를 위하여 표준화 공모전을 개최했다[1]. 4 라운드를 거쳐 2022년 7월에 표준화 알고리즘으로 4개의 알고리즘(격자3, 해시1)을 채택하였고, 격자 기반 암호에 집중됨으로써 벌어질 문제들에 대비하기 위하여 4라운드 후보 알고리즘 중 4개를 대체 알고리즘으로 추가 선정하였다. 이

중 3개는 코드기반 암호이고 1개가 아이소제니 기반 암호로, 아이소제니 암호에 해당하는 SIKE는 2022년 8월 보안 결함이 밝혀진 바 있다. 2022년 7월, 추가적으로 전자서명에 알고리즘에 대한 공모전을 시작하여 올해 8월 1라운드 진출자로 40개의 알고리즘이 공개되었고, 해당 공모전은 현재 진행 중에 있다.

국내에서는 국산 양자내성암호 알고리즘 개발을 위하여 2022년 KpqC 공모전을 개최하였다. 현재, 16개의 알고리즘이 1라운드 알고리즘으로 채택되었고 올해 12월 경, 1라운드 결과가 발표될 예정이다[2]. 2024년에 2라운드를 진행하여 최종 알고리즘을 선정할 계획이며, 선정된 알고리즘을 실제 현장의 적용에 고려되는 사항들을 논의하기 위해 3라운드 진행 여부를 검토하고 있다[3].

III. 양자내성암호 적용 동향

현재는 사용할 수 없지만 암호 분석와 관련된 양자컴퓨터인 CRQC에 따르면 이론적으로 현재 사용 중인 공개키 알고리즘을 깨뜨릴 수 있다. 현재는 읽을 수 없는 암호화된 데이터들을 저장하여 훗날 CRQC를 사용할 수 있게 되었을 때, 저장한 암호들을 해독하는 공격을 harvest-now-decrypt-later라 한다. 이를 방지하기 위해서 표준화 알고리즘이 발표된 후부터 기업들에서는 해당 표준화 알고리즘을 적용하고 있다. 본 장에서는 해당 양자내성암호 알고리즘을 적용한 사례들에 대해서 국외와 국내로 나누어 설명한다.

3.1 국외

구글의 경우 2016년 당시 양자내성암호 표준과 공모전 Round 2 후보였던 NewHope 격자기반 알고리즘과 TLS에서 키 합의에 널리 사용되는 타원곡선 알고리즘인 X25519를 결합하여 구글의 테스트용 브라우저인 크롬 카나리아(Canary)의 TLS에 적용하였다. 이때 개발한 양자 내성 키 합의 프로토콜을 CECPQ1 (combined elliptic-curve and post-quantum 1)라 지칭한다[4]. 2019년에 나온 CECPQ2는 NewHope 대신 NTRUHRSS를, CECPQ2b는 SIKE를 적용한 것이다. Cloudflare와 함께 실험을 진행한 결과, 다양한 네트워크 제품들이 구현한 양자 내성 TLS와 호환이 되지 않는 것을 확인하였고, 2023년 4월에 크롬 지원을 중단하였다[5]. 해당 실험 결과들에 기반하여 올해 8월, 크롬 116에서 X25519와 양자내성암호인 Kyber768을 결합한 하이브리드 키 캡슐화 메커니즘(KEM) X25519Kyber768을 제공하였다[6]. 이는 X25519의 키를 Kyber768 캡슐화 계층으로 둘러싸는 방식으로 수행된다.

AWS도 TLS에 양자내성암호를 적용한 프로토콜 s2n-tls가 있다. AWS도 구글과 마찬가지로 양자내성암호와 기존의 타원곡선 기반 암호인 ECDH를 결합한 형태의 하이브리드 양자 내성 TLS를 제공하였다. NIST PQC 공모전이 진행되는 중에는 CRYSTALS-Kyber, SIKE, BIKE를 제공하였지만, NIST PQC 공모전이 끝난 후에는 최종 선정 알고리즘인 Kyber만 제공하고 있다. s2n-tls는 암호화 키를 생성 및 제어를 제공하는 KMS(Key Management Service)와 SSL/TLS 인증서 관리를 제공하는 ACM(AWS Certificate Manager), 그리고 데이터베이스의 자격을 증명하고 API 키와 기타 보안 암호들의 관리를 제공하는 AWS Secret Manager 서비스에서 사용된다[7].

IBM은 IBM Cloud에서 암호화 키를 관리하는 서비스인 Key Protect에 요청을 보낼 때, TLS 연결 중 키를 보호하기 위해 Kyber를 적용하였다. 제공되는 사용모드는 ECDH의 적용 여부에 따라 두 가지로 나뉜다[8]. 첫 번째 하이브리드 모드로 ECDH와 Kyber를 결합한 것으로, 키 크기별로 세 가지 매개변수를 제공한다. 세 가지 매개변수 중 가장 낮은 L1의 보안을 제공하는 p256_kyber512는 p_256 곡선을 사용하여 kyber512과 ECDH를 결합한 것을 의미한다. 두 번째는 Kyber를 온전히 제공하는 양자 안전 모드이다. 이 또한 키 크기별로 세 가지 매개변수를 제공한다. IBM은 언급한 기업들 중 유일하게 하이브리드가 아닌 양자내성암호만 적용한

TLS를 제공한다는 이점을 가진 반면, 리눅스에서만 해당 기술을 사용할 수 있다는 한계점을 갖는다.

3.2 국내

LG 유플러스는 국내에서 양자내성암호 개발 및 적용에 유리한 고지를 선점하고 있다고 평가된다. 2020년 6월 코위버의 광전송장비(ROADM)에 양자내성암호 기술 탑재에 성공한 이후, 2022년 4월에 세계 최초로 PQC 전용회선 서비스(PQC전송장비)를 출시하였다[9]. 또한, 같은 해 9월 국내 최초로 eSIM에 양자내성암호와 하드웨어 물리적 복제 방지기능(PUF)을 탑재한 PQC PUF-eSIM를 선보였고, 10월에 개발된 PQC (PUF) VPN 기술을 응용하여, 암호화된 VPN을 구현하는 통신 프로토콜인 와이어가드에 PQC를 결합한 기술을 U+지능형 CCTV에 적용하기도 하였다. 현재 LG U+의 다양한 서비스들에 적용된 양자내성암호는 국내에서 서울대 Cryptolab에서 개발한 Rlizard로 이는 NIST 표준과 공모전 2라운드에서 보안강도가 검증된 격자 기반 알고리즘이다. 추후 KpqC 표준화가 완료되면 선정된 알고리즘으로 교체할 계획이라 명시하였다.

광전송장비 전문기업인 우리넷은 올해 7월, 패킷광전송장비(POTN)에 양자내성암호 Kyber를 적용해 상용화에 성공했다 발표하였다. 이를 통해 보안 전송 서비스를 확대할 수 있을 것으로 기대하고 있다.

[표 2] 최근 양자내성암호 적용 사례

	기업명	알고리즘	적용 내용
국외	구글	CRYSTALS-Kyber + ECDH	Chrome 116 (X25519Kyber768)
	AWS		KMS, ACM, AWS Secret Manager (s2n-tls)
	IBM		IBM Cloud (하이브리드 모드)
		CRYSTALS-Kyber	IBM Cloud (양자 안전 모드)
국내	우리넷		패킷광전송장비
	LG U+	Rlizard	PQC 전송장비, PQC PUF-eSIM, PQC VPN 등

[표 2]는 최근 국내외 양자내성암호 적용 사례들을 표로 정리한 것이다.

IV. 결론

본 논문에서는 기업에서 양자내성암호를 적용한 사례들을 국내, 국외로 나누어 살펴보았다. 국외의 사례들은 대부분 TLS에 사용되는 타원곡선 암호 알고리즘의 전환에 주로 사용되었다. 국외의 세 기업 모두 양자내성암호로 CRYSTALS-Kyber를 사용하였고, 대부분의 기업이 호환을 위하여 기존의 암호와 양자내성암호를 결합한 하이브리드 형태로 제공하였다. IQT Research는 세 번째 PQC 분석 보고서에서 2032년까지 PQC의 수익이 67억 달러(한화 약 8조 9천억원)까지 증가할 것이라 예측하였다. PQC에 대한 중요성이 커짐에 따라 기업에서 기존의 암호 대신 양자내성암호를 적용하는 사례가 증가할 것으로 예상된다.

국내에서는 우리넷이 Kyber를 적용하였고, 다양한 기술들에 양자내성암호를 적용해온 LG 유플러스의 경우 국내 양자내성암호인 Rlizard를 적용하며 KpqC 상용화에 앞장섰다. 올해 7월, 정부가 발표한 양자내성암호 전환을 위한 마스터플랜에 따르면 2035년까지 국내 암호체계들을 양자내성암호로 전환하는 것을 목표로 두고 있다. 이에 맞춰 국내에서도 양자내성암호에 대한 중요성이 더 커지며 기업에서 양자내성암호를 적용하는 사례가 증가할 것이라 기대된다.

V.Acknowledgement

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 50%) and this work was supported by Institute for Information & communications Technology Promotion(IITP)

grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%).

[참고문헌]

[1] NIST Post-Quantum Cryptography Project, https://csrc.nist.gov/Projects/post-quantum-cryptography.

[2] 양자내성암호연구단, https://kpqc.or.kr/competition.html, 2023년 8월.

[3] 이나리, 정경철, 지성택, 한 대완, "양자내성암호 국가공모전" 정보보호학회지 33, 3, 7-14, 2023년 6월.

[4]M.Braithwaite, Experimenting with post-quantum cryptography, https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html, July 2016.

[5] K.Kwiatkowski, L.Valenta, https://blog.cloudflare.com/the-tls-post-quantum-experiment, November 2019.

[6] Google, https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html, August 2023.

[7] P.Kampanakis, A.Volanis, G.Ravago, and T.Hansen, https://aws.amazon.com/ko/blogs/security/post-quantum-hybrid-sftp-file-transfers-using-aws-transfer-family, Jun 2023.

[8] IBM, https://cloud.ibm.com/docs/key-protect?topic=key-protect-quantum-safe-cryptography-tls-introduction, February 2022.

[9] LG U+, https://www.lguplus.com/biz/all/telecom/phones/quantum/B000000123.