Post-quantum 으로의 마이그레이션 조사

송경주 [1], 장경배 [1], 김현지 [1], 양유진 [1], 임세진 [1], 서화정 [1]
[1] 한성대학교 IT 융합공학부
thdrudwn98@gmail.com, starj1023@gmail.com, khj1594012@gmail.com, yujin.yang34@gmail.com,
dlatpwls834@gmail.com, hwajeong84@gmail.com

Investigate the migration process to post-quantum

Gyeong-Ju Song[1], Kyung-Bae Jang[1], Hyun-Ji Kim[1], Yu-Jin Yang[1], Se-Jin Lim[1], Hwa-Jeong Seo[1]
[1]Dept. of IT Convergence Engineering, Han-Sung University

요 약

대규모 양자컴퓨터의 개발은 현재 사용하는 많은 암호화 알고리즘에 위협이 될 것으로 예상한다. 현재 NIST 는 양자 후 시대에 대비하기 위해 양자 내성 암호를 표준화 하기 위한 작업을 진행하고 있으며 이에 따라 post-quantum 시스템의 마이그레이션 과정이 필요하며 각 시스템에 QSC 적용을 위한 연구들이 이어지고 있다. 본 논문에서는 양자 후 시대에 대비하기 위해 NIST 의 PQC post quantum conference 에서 발표한 PQC 후보와 QSC 마이그레이션 과정 및 적용 방안에 대해 조사한다.

1. 서론

최근 정보화 시대로 바뀌면서 데이터들이 클라우드 및 데이터 베이스 등 전자적으로 저장되어 관리되고 있다. 그 결과 인터넷, 모바일, IoT 등 모든 분야에 널리 사용 되고 있는 암호의 중요성이 크다[1].

양자컴퓨터는 빠르게 개발되고 있는 분야이며 대형 양자 컴퓨터가 개발되면 현재 사용하는 암호들이 양자 알고리즘에 의해 더이상 안전하지 않다는 것이 널리 알려져 있다. 양자 알고리즘 중 하나인 Grover's algorithm 은 정렬되지 않은 데이터 베이스에서 특정 데이터 찾는 속도를 높여 대칭키 암호에 위협이 되며, Shor's algorithm 은 다항 시간 안에 인수분해를 수행하여 공개키 암호에 위협이 된다[2][3]. 그 결과 양자 후 암호의 안정성을 평가하기 위해 양자 알고리즘을 사용한 암호 공격을 수행하고 필요한 양자 자원을 추정하는 연구들이 꾸준히 발표되고 있다 [4][5][6][7][8][9][10].

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 있으며 이에 따라 현재 사용하는 non quantum-safe 한 시스템을 quantum-safe 로 전환하는 과정에 대한 연구가 진행되고 있다. 본 논문에서는 양자 내성 암호(PQC)와 quantum-safe cryptography(QSC)의 마이그레이션을 위한 과정 및 사례를 조사한다.

2. Post-quantum cryptography(PQC)

NIST 에서는 안전한 PQC 표준을 정하는 것을 목표로 총 3 라운드의 post quantum conference 을 진행하였다. PQC 의 후보로는 크게 격자 기반, 코드 기반, 해시 기반, 다변수 기반, 아이소제니 기반이 있다. 후보 암호는 각 quantum-safe 한 문제로 안전성을 보장한다.

격자 기반은 NP-hard 기반의 안전성을 가진다. 다양한 응용 환경이 지원되고 구현 속도가 빠르고 변수 설정이 어렵다. 코드 기반은 알려지지 않은 오류 수정 코드를 디코딩 하는 문제를 기반으로 안전성을 가진다. 암복호화가 빠르지만 키 사이즈가 크다. 다변수 기반은 많은 변수로 이루어진 함수 식을 계산하는 것이 어렵다는 문제에 기반하며 서명 크기가 작고 계산 속도가 빠르지만 키 사이즈가 크다. 아이소제니 기반은 타원 곡선의 아이소제니 연산 문제를 기반으로 한다. 구현이 편리하고 키 사이즈가 작지만 연산 속도가 느리다. 해시 기반은 해시 함수의 collision resistance 문제에 기반한다. 안전성 증명이 가능하고 키 사이즈가 크다.

2020 년 7 월 22 일 NIST 는 <표 1>, <표 2>와 같이 7 개의 finalist 와 8 개의 alternate 를 발표했다. PQC finalist 알고리즘으로는 다변수 기반의 Rainbow, 코드 기반의 Classic McEliece, 격자 기반의 NTRU, CRYSTALS-KYBER, SABER, CRYSTALS-DILITHIUM, FALCON 이 있으며 PQC alternate 알고리즘으로는 격자기반의 FrodoKEM, NTRU-Prime, 아이소제니 기반의 SIKE, 코드기반의 HQC, BIKE, 다변수 기반의 GeMMS, 해시 기반의 SPHINCS+, 영지식 증명 기반의 Picnic

이 있다.

<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	

3. Quantum-safe cryptography(QSC) 마이그레이션 과정

3.1. QSC 마이그레이션 전환 단계

Non-QSC 에서 QSC 로 전환하는데 필요한 과정은 인벤토리(시스템) 편집, 마이그레이션 계획 작성, 마이그레이션 실행 순서로 진행된다[11].

인벤토리(시스템) 편집은 시스템에서 암호화 자산 및 프로세스를 식별하고 마이그레이션 대상이 암호화하는 엔티티 및 기능을 식별한다.

마이그레이션 계획 작성에서는 자산의 전체 목록과 자산에 대한 정보를 기록한다. 이때, 공개키 및 대칭키 암호로 암호화된 자산은 각각 마이그레이션 이후에도 동일한 방식으로 암호화 된다. 마이그레이션 과정에서 quantum-safe 암호는 더 큰 공개키 및 서명을 포함하므로 PKI 의 기능이 QSC 를 처리할 수 없는 경우 교체해야 하며 QSC 로 업그레이드 된 PKI 에는 quantum-safe 서명이 포함된 새로운 인증서가 필요하다. 또한 업데이트 된 PKI 의 엔티티에 대한 cryptographic agility(암호 민첩성)을 고려하여 추후 quantum-safe 알고리즘의 취약점이 발견되면 다른 quantum-safe 알고리즘으로 수정 및 전환하여 취약점을 해결할 수 있도록 해야 한다.

마이그레이션 실행은 인벤토리 편집, 마이그레이션 계획 작성에서 계획한 것을 구현하는 단계이다. 계획의 실행 가능성을 결정하기 위해 마이그레이션을 시뮬레이션 하고 테스트를 수행한다.

3.2. 양자내성암호 전환 과정 및 고려사항

United States Department of Homeland Security (DHS)은 NIST 와의 파트너십을 통해 양자 내성 암호 전환을 위해 조직이 취해야 하는 조치에 대한 로드맵을 만들었다[12]. 로드맵은 다음과 같이 7 단계로 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) 전환 계획

로드맵은 post-quantum 시대에서 데이터의 지속적인 보안을 보장하며 새로운 양자 내성 암호화 표준으로 전환하는 준비를 위한 계획 수립에 도움이 될 것이라 기대한다.

양자 내성 암호 알고리즘 선택을 위한 고려사항으로는 보안, 알고리즘 구현의 특성, 성능 등이 있다. 보안은 충분한 security level 을 제공하는지, 신뢰성 있는 보안 증명인지 등을 고려한다. 알고리즘 구현의 특성으로는 부채널 저항성, 유연성 등이 있으며 성능으로는 매개변수의 크기, 키생성 및 암복호화, 서명 및 검증 속도 등이 있다. 새로운 알고리즘은 키 크기, 서명 크기, 오류 처리 속성 등에 따라 성능 및 안전성에 영향을 미칠 수 있어 이에 대한 대비 또한 필요하다[13][14].

4. Quantum-safe cryptography(QSC) 적용 방안[1]

4.1. Network security protocols

두 대상이 네트워크를 통해 안전하고 인증된 통신 링크를 설정하려고 할 때, 한쪽 혹은 양쪽은 통신 하고자 하는 상대방의 Public Key Infrastructure(PKI)에서 서명된 인증서를 얻는 방식을 사용한다. 하지만 대부분의 공개키 기반 통신은 대규모 양자컴퓨터에 의해 취약해질 수 있기 때문에 양자에 안전한 공개키 기반 handshake protocol 에 대한 연구가 집중되고 있다.

4.1.1. TLS(Transport Layer Security) cryptography

TLS 는 컴퓨터 네트워크를 통해 통신 보안을 제공

하는 암호화 프로토콜로서 웹 클라이언트와 서버 간에 교환되는 데이터를 보호한다.

양자컴퓨터가 발전함에 따라 추후 현재 사용하고 있는 TLS 통신 알고리즘이 깨질 위험이 있다. TLS 는 키 설정 및 인증 서비스를 위해 PKI 가 지원하는 공개키 암호를 광범위하게 사용하며 이를 quantum-safe 하게 업데이트 하는 것이 필요하다. TLS 는 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-safe 로 쉽게 바꿀 수 있으므로 공개키에 초점을 맞추고 있다.

TLS 에 양자 내성을 적용한 방법으로 Drop-in replacement, Hybrid scheme, Re-engineering 등이 있다. Drop-in replacement 는 가장 간단한 제안으로, 현재 공개키 일부 또는 전체를 유사한 quantum-safe drop-in replacement 로 교체하는 방식이다. Hybrid scheme 은 신뢰할 수 있는 기존 key agreement scheme(키 합의 방식)와 새로운 quantum-safe agreement scheme 의 출력에서 암호화 키를 파생시키는 hybrid 방식이다. 이 방식은 quantum-safe 암호 변경의 중간 단계로 볼 수 있으며 추가 기능 및 보안을 제공한다. Re-engineering 방식은 인터넷 인프라를 재설계하고 시스템 엔지니어링 접근 방식을 사용하여 성능 문제를 완화하고 더 큰 key 크기를 처리할 수 있도록 하는 방식이다.

4.2. 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 replacement 로 전환하는 방법이 적합하다. 오프라인은 온라인 보다 속도 및 대역폭이 비교적 자유롭기 때문에 hash-tree 서명이 잠재적인 대안으로 제안된다.

5. 결론

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

6. Acknowledgement

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 100%).

참고문헌

[1] ETSI, “Quantum Safe Cryptography; Case Studies and Deployment Scenarios” [internet], https://www.etsi.org/deliver/etsi_gr/qsc/001_099/003/01.01.01_60/gr_qsc003v010101p.pdf

[11] ETSI, “CYBER; Migration strategies and recommendations to Quantum Safe schemes” [internet], https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[13] NIST, “Towards PQC Standardization and Migration” [internet],https://icmconference.org/wp-content/uploads/Pre-ICMC-Chen-08122020-.pdf

[14] NIST, “Considerations in Migrating to Post-Quantum Cryptographic Algorithms” [internet], https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

[12] DHS, “Preparing for Post-Quantum Cryptography: Infographic”[internet],“https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf”

[2] Grover, Lov K. "A fast quantum mechanical algorithm for database search." Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996.

[3] Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994.

[4] Anand, R., Maitra, A., Mukhopadhyay, S.: Grover on SIMON. Quantum Information Processing 19(9) (2020) 1–17

[5] Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R.: Applying Grover’s algorithm to AES: quantum resource estimates. In: Post-Quantum Cryptography, Springer (2016) 29–43

[6] Jang, K., Choi, S., Kwon, H., Kim, H., Park, J., Seo, H.: Grover on Korean block ciphers. Applied Sciences 10(18) (2020) 6407

[7] Song, G., Jang, K., Kim, H., Lee, W.K., Seo, H.: Grover on Caesar and Vigen`ere ciphers. IACR Cryptol. ePrint Arch. 2021 (2021) 554

[8] Langenberg, B., Pham, H., Steinwandt, R.: Reducing the cost of implementing AES as a quantum circuit. Technical report, Cryptology ePrint Archive, Report 2019/854 (2019)

[9] Jang, K., Song, G., Kim, H., Kwon, H., Kim, H., Seo, H.: Efficient implementation of PRESENT and GIFT on quantum computers. Applied Sciences 11(11) (2021) 4776

[10] Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing Grover oracles for quantum key search on AES and LowMC. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer (2020) 280–310