클라우드 컴퓨팅 환경에서 양자내성암호 안전성 분석

송정규, 허준범*
고려대학교, *고려대학교
jgsong@isslab.korea.ac.kr, jbhur@korea.ac.kr

Survey on post-quantum cryptography in cloud computing

Song Jeong Gyu, Hur Jun Beom*
Korea Univ., *Korea Univ.

요 약

본 논문은 클라우드 기반 양자 컴퓨팅 리소스를 활용한 위협 시나리오를 이해함으로써 보안 위협이 되는 사례를 탐색하였다. 또한 기존 인터넷 서비스 제공업체 및 공급업체에서 제공하는 암호화 및 인증 수준을 Post-Quantum 암호 표준 후보와 비교한다.

Ⅰ. 서 론

양자 컴퓨터는 양자역학에서 양자 얽힘, 중첩, 텔레포테이션 등의 효과를 이용해 계산하는 컴퓨터이다. 비트를 사용하는 전통적인 컴퓨터는 0과 1을 이용하여 정보를 표현 하고 저장하지만, 양자 컴퓨터는 0과 1을 동시에 공존 시킬 수 있으며 이를 저장할 수 있는 정보 단위를 '큐빗(Qubit)'이라고 부른다. 양자 컴퓨터는 양자 정보를 제어하기 힘들고 들어가는 재료의 특성상 굉장히 고가의 장비로 일반적인 컴퓨팅 환경에서는 활용할 수가 없다. 그렇지만 대형 IT 업체들은 개발자들이나 고객들이 클라우드 서비스로 양자 컴퓨터를 시뮬레이션 할 수 있는 플랫폼을 제공하고 있다.

첫번째로 IBM QX[6]는 퀀텀 랩 서비스를 통해서 실행 가능한 주피터 노트북으로 코드, 방정식, 시각화, 설명문을 결합한 스크립트를 작성할 수 있다. Qiskit(퀴스킷)이라는 오픈 소스 기반의 양자 소프트 웨어 프레임 워크를 제공하며 양자 컴퓨팅에 필요한 회로 조합 및 시뮬레이팅을 GUI 형태로도 구현 할 수 있게 해준다.

두번째로 MS Azure Quantum[7]은 프로그래머가 시뮬레이션으로 구현된 양자 하드웨어나 실제 양자 하드웨어에서 양자 코드를 동작 할 수 있다. 퀀텀 개발 키트라는 오픈 소스 개발 도구를 제공하고 있는데 양자 프로그램 언어인 Q#, 라이브러리 세트, 시뮬레이터, VS code(Q# 지원), 주피터 노트북과 .Net, 파이썬 등과의 상호 운용을 할 수 있도록 지원한다.

마지막으로 Amazon Braket[3]은 양자 컴퓨팅을 시작할 수 있는 관리형 서비스로 빌드, 테스트, 런 3개의 모듈로 구성되어 있다. 빌드 모듈에서는 주피터 노트북을 통해 브라켓 SDK, 샘플 알고리즘, 리소스, 개발자 도구로 사전 구성되어 있다. 실험 모듈에서는 고성능 양자 회로 시뮬레이터에 대한 접근을 제공하고, 실행 모듈에서는 온디맨드 액세스를 여러 종류의 양자컴퓨터 형태로 제공한다.

오늘날 현대 암호 알고리즘은 수학적 지식을 기반으로 설계되어 소스 코드 형태로 구현되었으며, 이를 고전 컴퓨터들의 연산장치들을 이용하여 계산하는 방식이다. 현대 암호 알고리즘은 정보보호의 키 분배, 인증, 전자 서명 등의 서비스를 통해 정보보호의 기본적인 속성인 기밀성과 무결성, 상호 인증 및 부인방지 등을 만족한다다. 여기에서 사용되는 대표적인 암호 알고리즘으로는 소인수 분해 문제의 어려움을 기반으로 한 RSA[10]가 있다.

이 논문의 서론 이후 크게 세 개의 장으로 구성 되어 있다. 2장에서는 소인수 분해 문제를 다항시간 안에 풀 수 있는 Shor's 알고리즘[11]과 이를 클라우드 양자 컴퓨팅으로 구현한 사례[9]를 먼저 소개한다. 이에 따른 보안 위협을 대비하기 위한 NIST의 양자내성암호 알고리즘 후보[1]를 소개한다. 3장에서는 양자내성 암호 알고리즘이 적용된 실제 사례를 소개한다. 4장에서는 양자내성 암호 알고리즘의 보안 위협에 대해서 소개한다.

Ⅱ. 본론

A. 관련연구

1. 쇼어알고리즘

RSA 알고리즘은 소인수 분해 문제를 푸는 데 시간이 오래 걸린다는 어려움을 기반으로 하고 있다. P와 Q가 1이 아닌 서로 다른 소수이고 N = P * Q 라고 가정할 때. P와 Q를 알면 N을 구하는 것은 쉽지만 N만으로 소수인 P와 Q가를 구하는 것이 고전 컴퓨터로 계산하는 데 시간이 오래 걸린다는 점을 이용한다. 쇼어 알고리즘은 소인수 분해 문제를 푸리에 변환(Fourier Transform) 문제로 변형하여 풀 수 있다는 점에 착안 했다. 푸리에 변환은 함수의 주기성이 나타난다는 점을 이용하는데 쇼어 알고리즘을 적용하여 고전 컴퓨터로 소인수 분해를 계산할 경우 주기 r을 찾는 계산이 전체 계산시간의 대부분을 차지한다. 양자 컴퓨터는 그림 1과 같이 QFT(Quantum Fourier Transform) 회로를 구성하여 이 문제를 최적화 할 수 있다.

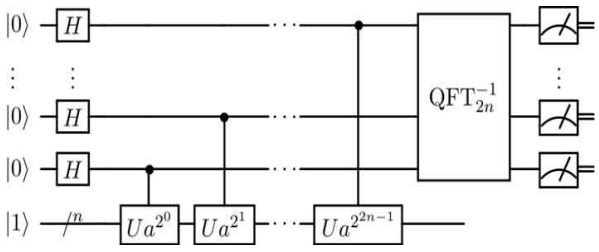

Fig. 1.QFT circuit
그림 1.QFT 회로.

2. 쇼어알고리즘의 구현

쇼어 알고리즘 발표된 이후 QFT circuit을 이용하여 구현한 논문들이 있다[12, 13]. 클라우드 양자 컴퓨팅을 활용하여 구현한 Vaishali Bhatia의 논문[9]에서는 쇼어 알고리즘의 QFT를 IBM Qiskit을 이용하여 구현하였다.

고전 컴퓨터에서 구현하고 계산한 쇼어 알고리즘의 시간복잡도가 $\exp(3\ \ 64/9n(\log n))$인데 비해 양자 컴퓨터를 활용한 경우 $O(n^3\log n)$로 줄어든 것을 확인하였다. 클라우드 양자 컴퓨팅을 이용하여 쇼어 알고리즘을 최적화하고 RSA에 대한 공격이 실세계에서 실현 가능하다는 것을 증명하였다.

3. 양자내성암호 후보

양자 컴퓨터를 이용한 공격이 실현 가능함에 따라 RSA 알고리즘이 근미래에 암호학적으로 안전하지 않을 것을 대비하기 위해 미국의 국립표준기술연구소(NIST, National Institute of Standards and Technology)는 Post-Quantum Cryptography Standardization[1] 을 통해 양자 컴퓨팅을 이용한 공격에 내성을 갖는 암호 후보를 [표 1]과 같이 심사하고 있다[2]. 표준화 작업은 2020년을 기준으로 3라운드까지 진행 되었다. NIST는 암호 후보를 2022년에서 2023 년 내에 선정할 예정이다.

표 1. NIST 양자 내성 암호 3라운드 후보
Table 1. NIST PQ-crypto-algorithms 3rd round candidates

	최종 후보	대체 후보*
KEMs/ Encryption	Kyber NTRU SABER Classic McEliece	Bike FrodoKEM HQC NTRUprime SIKE
Sigantures	Dilithium Falcon Rainbow	GeMSS Picnic SPHINCS+

* 대체 후보는 3라운드 최종 후보에서 탈락된 경우 4라운드 후보에 포함될만한 후보.

B. 사례 분석

2021년을 기준으로 아직까지 양자내성암호 표준화가 진행되지 않았다. 이는 각 알고리즘의 기반이 되는 이론에 따른 장점과 단점이 있으며 알고리즘의 소스코드가 계속 업데이트 되고 있기 때문이다. 하지만 표준이 지정되지 않았다고 하더라도 실세계에서 사업을 하고 있는 회사들은 각자 다른 수학적 이론을 적용한 자체 암호 시스템이나 NIST의 양자내성 암호 후보를 참고하여 보완책을 마련하고 있다. 이 논문에서는 두 가지 사례를 예시로 들고자 한다.

1. Cloud Flare

Cloud Flare는 TLS를 핸드셰이크 서명에 대하여 환경별로 적합한 양자내성 암호 알고리즘을 선정하였다. 온라인에서는 속도가 빠른 Dilithium을 사용하는 것이 좋다. 공개 키가 오프라인으로 적용될 때 Falcon을 사용하는 것이 적절하다. 마지막으로 공개 키가 오프라인으로 적용되지 않는 경우(예: SCT와 OCSP 스테이플에서 사용되는 경우) Rainbow 알고리즘을 적용하는 것이 알맞다고 분석하였다[4].

2. AWS(Amazon Web Services)

AWS는 2020년 2라운드 양자내성암호 들에 대하여 TLS 1.2 및 TLS 1.3 연결을 할 수 있도록 라이브러리를 지원하고 있다. 양자 내성 암호인 Kyber, BIKE, SIKE 등을ECDHE와 결합하여 사용 할 수 있다[5, 14].

C. 양자내성암호 안전성 문제

양자내성암호 알고리즘을 현재 네트워크 시스템에 활용될 경우 고려해야하는 보안 위협 모델은 다음과 같다.

1. 부채널 공격(Side Channel Attack)

부채널 공격은 연산시 발생하는 타이밍 정보, 열, 전력 소모량 등의 부가정보들을 분석해서 암호키를 복구하는 공격 방법이다.

Amund Askeland and Sondre Rønjom의 논문[8]에서는 양자내성암호 후보 중 하나인 NTRU(격자기반암호)에 대하여 전력분석을 통한 부채널 공격을 실시, 복호화 코드를 구현하여 부분키 복구하였으며, lattice reduction을 통하여 전체 키를 복구하는 공격을 수행하였다.

2. 양자내성암호 알고리즘 미지원(PQC algorithm not supported)

TLS 핸드셰이크는 secure channel을 만들 때 어떤 암호 알고리즘을 사용할지 ChangeCipherSpec 단계에서 협의를 한다. 만약 클라이언트의 Client Hello 단계나 서버의 Server Hello 단계 중에서 협의를 위해 제공하는 암호 알고리즘 중에서 양자내성암호 라이브러리를 지원하지 않을 수 있다. 이 때 양자 컴퓨터 공격 내성 여부와 상관 없이 RSA 라이브러리를 이용할 수 있다.

3. 상수 시간 프로그래밍(Constant Time Programming)

양자내성암호 알고리즘 후보들은 네트워크 통신이 이뤄지는 구간에 대하여 Quantum Computing 자원을 이용한 공격에 대해서만 내성이 있음을 보장한다. 양자내성암호 알고리즘 후보들이 Cross-VM Cache Side-channel Attack과 같은 위협에 노출된 환경에 대해서도 내성이 있는지 확인되지 않았다. 따라서 양자내성암호 알고리즘 라이브러리가 Constant Time Programming 패러다임을 따르지 않는다면 얼마든지 취약점이 발견 될 수 있다.

Ⅲ. 결론

양자 컴퓨터가 업그레이드 되고 이와 관련된 클라우드 서비스의 접근성이 좋아질 경우 양자 컴퓨팅과 양자 알고리즘을 활용하여 소인수 분해 문제나 이산 대수 기반의 암호 알고리즘을 무력화 하는 공격이 현실로 다가올 것이다. 이 논문에서는 양자내성 암호 별도의 특성을 활용한 특별한 공격기법이 아닌 고전적인 컴퓨터에도 위협이 됐던 공격 사례들을 대상으로 보안 문제들을 제기하였다. 양자 컴퓨터가 발전하고 더 나아가 양자 통신을 기반으로 한 양자 인터넷 환경이 구축 되더라도 기존의 전통적인 컴퓨터 기반의 Legacy 네트워크 환경이 공존 할 수 있다[15]. 따라서 이에 대비하기 위한 보안 문제들을 지속적으로 탐구하고 확장하여 잠재적인 위험을 예방하는 것이 중요하다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원(No.2019-0-00533)과 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2021-0-01810)

참 고 문 헌

[1] 2020. NIST Post-Quantum Cryptography 3rd Round. Retrieved Jan., 13, 2022, from https://csrc.nist.gov/publications/detail/nistir/8309/final. (2020).
[2] 2020. NIST Post-Quantum Cryptography 3rd Round Lists Retrieved Jan., 13, 2022, from https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf. (2020).
[3] 2021. Amazon Braket. Retrieved Jan., 13, 2022, from https://aws.amazon.com/braket/. (2021).
[4] 2021.casestudy1Cloudflare. Retrieved Jan., 13, 2022, from https://blog.cloudflare.com/sizing-up-post-quantum-signatures/. (2021).
[5] 2021.casestudy2AWS. Retrieved Jan., 13, 2022, from https://aws.amazon.com/ko/blogs/security/round-2-post-quantum-tls-is-now-supported-in-aws-kms/. (2021).
[6] 2021. IBM Quantum eXperience.Retrieved Jan., 13, 2022, from https://quantum-computing.ibm.com/. (2021).
[7] 2021. MS Azure Quantum. Retrieved Jan., 13, 2022, from https://azure.microsoft.com/en-us/services/quantum/.(2021).
[8] Amund Askeland and Sondre Rønjom. 2021. A Side-Channel Assisted Attack onNTRU.IACR Cryptol. ePrint Arch.2021 (2021), 790.
[9] Vaishali Bhatia and K. R. Ramkumar. 2020. An Efficient Quantum Computingtechnique for cracking RSA using Shor's Algorithm.2020 IEEE 5th InternationalConference on Computing Communication and Automation (ICCCA)(2020), 89 - 94.
[10] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. 1983. A method forobtaining digital signatures and public-key cryptosystems.Commun. ACM26(1983), 96 - 99.
[11] Peter W. Shor. 1994. Algorithms for quantum computation: discrete logarithmsand factoring.Proceedings 35th Annual Symposium on Foundations of ComputerScience(1994), 124 - 134.
[12] Kapil Kumar Soni and Akhtar Rasool. 2018. Cryptographic Attack Possibilitiesover RSA Algorithm through Classical and Quantum Computation. In2018 Inter-national Conference on Smart Systems and Inventive Technology (ICSSIT).
11 - 15.https://doi.org/10.1109/ICSSIT.2018.8748675
[13] Yahui Wang, Huanguo Zhang, and Houzhen Wang. 2018. Quantum polynomial-time fixed-point attack for RSA.China Communications15, 2 (2018), 25 - 32.https://doi.org/10.1109/CC.2018.83002
[14] 2021. Matthew Campagna, An AWS approach to post-quantum cryptography w/AWS Sr Principal Eng & Cryptographer(2021) Retrieved Jan., 13, 2022, from https://www.youtube.com/watch?v=ixn3A7htBnw
[15] Kwangseok Seok Noh, Heo Jun. Proceedings of Symposium of the Korean Institute of communications and Information Sciences , 2021.6, 630-631