양자컴퓨팅과 양자내성암호

서화정 한성대학교 융합보안학과 교수

1. 머리말

현대인들이 사용하는 기존 컴퓨터의 경우 0과 1로 대표되는 비트(bit) 단위 연산을 지원한다. 반면에 양자컴퓨터는 0과 1을 동시에 가지는 중첩 상태를 표현하는 큐비트(qubit) 단위 연산을 지원하며 현시대의 특정 난제를 해결할 수 있는 컴퓨팅 능력을 가지고 있다. 하지만 해당 난제 중에는 암호화 연산의 기반 문제와 같이 해결되어서는 안되는 문제도 포함된다. 따라서 암호학계에서는 양자컴퓨터 시대에 대한 대비를 2017년부터 NIST 양자내성암호 공모전을 기점으로 본격화하고 있다. 본 고에서는 양자컴퓨터의 개발 현황, 양자컴퓨팅을 지원하는 양자컴퓨터 플랫폼, 그리고 양자내성암호에 대한 최신 동향에 대해 확인해 보도록 한다.

2. 양자컴퓨터의 발전과 역사

2.1 양자컴퓨터의 개발

양자컴퓨터 개발에 있어 가장 선두 그룹으로는 IBM이 있다. 매년 IBM에서는 양자컴퓨터 개발로드맵을 <표 1>과 같이 제시하고 있다. 해당 로드맵에 따른 최근의 발표는 2022년 11월 9일에 있었으며 이는 433큐비트 Osprey 양자컴퓨터에 대한 내용이다[1]. IBM에서는 단일칩의 한계를 넘어서기 위해 양자칩을 다수로 연결하는 병렬화 방식을 통해 대규모 양자컴퓨팅 환경을 구축하는 것을 목표로 하고 있다[3].

<표 1> IBM의 양자컴퓨터 개발 로드맵[2]

Year	2019	2020	2021	2022	2023		2024		2025	2026
Proce-ssor	Falcon	Humming bird	Eagle	Osprey	Condor	Heron	Flamingo	Crossbill	Kooka-burra	Scaling
Qubit	27	65	127	433	1,121	133	1,386	408	4,158	10k~100k

다만 IBM의 양자컴퓨터 개발 로드맵에서 한가지 간과하고 있는 사실이 있다면 대규모 양자 컴퓨팅 시에는 많은 양자 에러가 발생하게 되며 이를 적절히 교정하지 못할 경우에는 정확한 연산 결과를 도출할 수 없다. 이러한 양자 에러와 밀접한 연관성이 있는 것이 바로 양자회로의 깊이(depth)이다. 동일한 큐비트를 쓰는 경우에도 양자상태를 유지해야 하는 시간에 해당하는 회로의 깊이가 길어질수록 양자 오류는 증가하게 되고 이를 수정하기 위한 오류 정정(Quantum error

correction) 기술 발전이 점차 중요해지게 된다[4].

2.2 양자컴퓨팅 플랫폼

양자컴퓨팅 플랫폼은 양자컴퓨터 자원을 사용해서 양자 응용 프로그램을 구현 및 실행할 수 있도록 하는 서비스를 의미한다[5]. 아래에는 양자컴퓨팅 플랫폼을 살펴보도록 한다.

IBM Qiskit은 IBM에서 개발한 오픈소스 플랫폼으로, Jupyter Notebook과 연동한 Python 및 OpenQASM(Open Quantum Assembly Language)를 활용한 양자 알고리즘 구현이 가능하다. 특히 국내에서 양자컴퓨팅 대회를 주기적으로 개최하며 활발히 Qiskit에 대한 대외홍보를 진행해나가고 있다[6]. Goolge Cirq는 Google Quantum AI에서 제공하는 오픈소스 프레임워크이다. 기본적으로 Cirq는 Python 기반으로 동작하며, 회로 테스트를 위한 파동함수, 밀도 매트릭스용 시뮬레이터를 포함하고 있다[7]. ProjectQ는 취리히 공과대학교 연구팀에서 개발했으며 Amazon Braket, Azure Quantum, IBM Qiskit, IonQ 등의 외부 플랫폼에 대한 백엔드를 지원한다[8]. Amazon Braket은 양자 하드웨어를 제공하는 업체가 보유한 양자 자원 및 기술을 사용할 수 있다. Python을 기반으로 동작하며, Jupyter Notebook을 활용할 수 있다[9]. Azure Quantum은 Microsoft에서 제공하는 클라우드 양자컴퓨팅 서비스이다. Azure Quantum은 자체적으로 제공하는 개발 도구인 QDK(Quantum Development Kit)를 사용하며, Jupyter Notebook과 연동해서 Azure Quantum 서비스를 제공한다[10]. Intel Quantum SDK는 양자 소프트웨어 개발 키트로 LLVM(Low Level Virtual Machine) 컴파일러를 사용하여 C++를 지원하기 위해 개발되었다[11].

2.3 양자컴퓨터와 현대 공개키 암호의 위기

대표적인 현대 공개키 암호화 알고리즘인 RSA와 ECC는 소인수분해와 이산대수 문제에 기반하여 안전성을 보장하고 있다. 하지만 양자컴퓨터 상에서 동작하는 Shor 알고리즘을 사용할 경우 기존에 난제로 생각되었던 해당 문제들을 다항 시간 내로 해결하는 것이 가능하다[12]. 예를 들어 RSA의 경우 보안강도에 해당하는 비트의 약 2배에 달하는 큐비트와 이에 대응되는 Shor 알고리즘의 회로 depth를 안정적으로 수행할 수 있는 양자컴퓨팅 기술이 가능할 경우 RSA 해킹이 가능해진다. 점차 가시화되어가고 있는 고성능 양자컴퓨터 환경에 대비하기 위해서는 기존의 공개키 암호화 시스템이 아닌 양자 내성을 가진 암호로의 전환이 요구되고 있는 시점이다.

3. 양자내성암호의 등장

3.1 NIST의 양자내성암호 공모전과 벤치마크

양자컴퓨터가 현행 암호 시스템을 붕괴시킬 우려가 커지자, 2017년 초 미국 NIST(National Institute of Standards and Technology)에서는 양자내성암호 공모전을 개최하였다. 해당 공모전은 총 3번의 심사과정을 거쳐 2022년 1차 표준화 양자내성암호화 알고리즘을 선정하였다. 1차 표준화 알고리즘은 총 4종류이며, 키교환 알고리즘에는 CRYSTALS-Kyber[13] 그리고 전자서명 알고리즘으로는 CRYSTALS-Dilithim[14], Falcon[15], 그리고 SPHINCS+[16]가 선정되었다. 다만 키교환 알고리즘은 격자기반 하나에만 의존할 수 없기에 추가적으로 BIKE, Classic McEliece, HQC, 그리고 SIKE 중에서 선정작업을 진행하는 중에 있다. 다만 SIKE의 경우 glueand-split 정리를 사

용한 키 복구 공격으로 다항시간 내로 키가 복구되는 취약점이 발견됨으로써 현재 후보군에서 제외되었다[17].

NIST에서는 이와는 별개로 추가적인 전자서명 표준 선정을 위한 공모전을 진행하는 중에 있다[18]. 1차 표준 알고리즘들이 격자 기반에 치우쳐 있기 때문에 다른 기반 문제를 선정하기 위한 움직임으로 사료된다. <표 2>는 추가 서명 공모전 1라운드의 후보 알고리즘 목록이다. 공모전의 1라운드 후보는 2023년 7월 17일에 발표되었으며 일부 알고리즘(3WISE[19], EagleSign[20], KAZ-SIGN[21], Xifrat1-Sign.I[22])은 발표 직후 많은 취약점이 보고되었다.

<표2> NIST 추가 서명 공모전의 1라운드 후보 알고리즘

Scheme	Algorithms
Code	CROSS, Enhanced pqsigRM, FuLeeca, LESS, MEDS, Wave
Isogeny	SQIsign
Lattice	EagleSign, EHTv3 and EHTv4, HAETAE, HAWK, HuFu, Raccoon, SQUIRRELS
MPC-in-the-Head	Biscuit, MIRA, MiRitH, MQOM, PERK, RYDE, SDitH
Multivariate	3WISE, DME-Sign, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX
Symmetric	AIMer, Ascon-Sign, FAEST, SPHINCS-alpha
Other	ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Preon, Xifrat1-Sign.I

양자내성암호의 실용화 관점에서 살펴볼 때 컴퓨터 상에서의 연산 효율성은 매우 중요하다. 따라서 각 알고리즘의 효율성과 구현 적합성을 확인하기 위해 PQClean, pqm4와 같은 프로젝트가 함께 진행되었다. PQClean 프로젝트는 NIST 양자내성암호 후보 알고리즘의 구현 적합성 확인 및 성능 측정을 위한 프로젝트이다[23]. 해당 프로젝트에서는 모든 알고리즘의 소스코드를 분석하며 구현상의 문제점을 분석하였다. 이는 알고리즘이 가지는 취약점이 없더라도, 구현이 잘못되었다면 다른 유형의 취약점으로 이어질 수 있기 때문이다[24]. pqm4는 임베디드 장비에 국한된 벤치마크 플랫폼으로써 32-비트 ARM Cortex-M4 상에서 양자내성암호 알고리즘의 구현을 점검하고 성능을 측정한 라이브러리이다[25]. 32-비트 ARM Cortex-M4를 대상으로 한 이유는 NIST의 양자내성암호 벤치마크 요구사항에서 제시되었으며 저전력 프로세서이기 때문에 양자내성암호의 임베디드 포팅 여부를 가늠하는 방안으로 적합하기 때문이다.

3.2 한국형 양자내성암호 표준화 공모전 KpqC

양자내성암호에 대한 관심이 높아짐에 따라, 한국에서도 자체적인 표준 선정을 위한 양자내성암호 공모전 KpqC를 개최하여 현재 운영 중에 있다. KpqC에서는 크게 국내 양자내성암호 기술력 제고 및 저변 확대, 양자내성암호 분야의 인력 양성, 산·학·연·관의 협업으로 선제적 기술 개발, 그리고 양자내성암호 국가공모전 개최와 같은 목적을 지향하고 있다.

KpqC 공모전은 2022년 2월 18일까지 알고리즘 설계서를 제출할 수 있는 0라운드를 진행하였으며 1라운드는 2022년 12월에 발표되었다. 1라운드 진출 알고리즘은 총 16종류로, <표 3>과 같다. 제출된 PKE/KEM(Public Key Encryption/Key Encapsulation Mechanism) 알고리즘은 7개이며,

전자서명은 9개이다. 전체적으로 격자 기반 알고리즘이 많이 제출되었으며 그 다음으로는 코드 기반 알고리즘이 다수를 이루고 있다[26].

<표3> KpqC Round 1 진출 알고리즘

Scheme	Public Key Encryption Key Encapsulation Mechanism	Digital Signature
Code	Layered-ROLLO-I PALOMA REDOG	Enhanced pqsigRM
Lattice	NTRU+ SMAUG TiGER	GCKSign HAETAE NCC-Sign Peregrine SOLMAE
Multivariate	-	MQ-Sign
Isogeny	-	FIBS
Graph	IPCC	-
Zero-Knowledge		AIMer

이와 함께 원활한 KpqC 공모전 운영을 위해서 KpqC 토론 포럼이 제공되고 있다[27]. 해당 포럼에서는 국내외 양자내성암호 연구자들이 모여 KpqC 알고리즘을 검증하고 토의를 진행하고 있다. KpqC 공모전도 NIST의 양자내성공모전과 유사하게 벤치마크 플랫폼이 존재한다. KpqClean 프로젝트는 의존성이 제거된 라이브러리를 제공하며 Intel, Ryzen, ARM 프로세서를 대상으로 벤치마크를 진행한 결과를 제공한다. 또한 Valgrind 툴을 사용한 메모리 사용량, 메모리 누수, 상수 시간 구현을 점검한 결과물을 제공하고 있다[28].

4. 양자내성암호로의 전환

양자내성암호가 표준화된 이후에는 현행 암호시스템을 양자내성암호로 빠르게 전환해야 하는 이슈가 남아있게 된다. 암호화 알고리즘을 빠르게 전환하기 위해서는 기업 내의 암호화 알고리즘을 파악하고 암호화 인벤토리(cryptographic inventory)화 해야 한다. 메모리 성능 측면에서 양자내성암호는 기존 암호 알고리즘들에 비해 키사이즈와 암호문 그리고 서명의 크기가 매우 큰편이다. 이러한 양자내성암호의 특징은 실제 네트워크 서비스 상에서 큰 전송 부하로 이어질 수 있기에 이를 대비해야 한다. 기존 프로토콜 및 시스템과의 호환성을 고려하여 다양한 요구사항을 해결하는 것을 의미하며 단순히 현대 공개키암호를 양자내성암호로 교체하는 것을 의미하지 않는다.

미국의 NIST에서는 양자내성암호로 전환하는 과정에서 암호화 라이브러리, 검증 도구, 하드웨어, 운영체제, 응용 프로그램 코드, 통신 프로토콜과 같은 광범위한 부분에서 변경이 필요함을 명시하였다. 또한 이와 관련된 보안 표준, 절차, 모범 사례 문서들도 수정하고 교체해야 함을 알렸다. 특히 알고리즘 전환 시에 각 요소를 고려하고 평가 및 호환성 검토가 반드시 진행되어야 함을 강조했다.

미국의 국토안보부에서는 양자내성암호로 전환하는 데 긴급도(urgency), 범위(scope), 비용(cost), 기타(other factors), 우선순위(priority for assistance)를 고려하여 전환이 가장 시급한 분야를 선정했다[29]. 각 분야는 55개의 국가 중요 기능(National Critical Functions, NCFs)으로 분류했고, 가장 우선순위가 높은 것은 6개, 보통인 것은 15개, 낮은 것은 34개로 평가되었다. 우선순위가 높은 6개 기능은 인터넷 기반 콘텐츠 정보 제공 및 커뮤니케이션 서비스, 전기 분배, 민감한 정보보호, 전기 생성, 정보 기술 제품 및 서비스, 방위 재료 및 운영 지원 제공이 이에 속한다.
앞에서 살펴본 바와 같이 양자내성암호로의 전환은 전 세계적인 관심사이며 산학연이 함께 고민해야할 큰 숙제로 점차 다가오고 있다.

5. 맺음말

본고에서는 양자컴퓨터의 개발, 양자내성암호의 발전 그리고 양자내성암호 전환 이슈에 대해 확인해 보았다. 현재 양자컴퓨터의 발전은 가시화 되어가고 있으며, 암호학계에서는 혹시 모를 현대암호의 붕괴에 대비하고자 양자내성암호 개발에 박차를 가하고 있다. 아직은 해결해 나가야 할 이슈가 많은 상황이지만 산학연이 함께 관심을 가지고 연구하고 개발해 나간다면 양자컴퓨터에 대한 위협은 대비가 충분히 가능할 것으로 사료된다.

※ 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, 100%).

[참고문헌]

[1] IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two, IBM Newsroom, https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBMQuantum-System-Two
[2] IBM Quantum Computing | Roadmap, IBM, https://www.ibm.com/quantum/roadmap
[3] Castelvecchi, D. (2023). Underdog technologies gain ground in quantum-computing race. Nature.
[4] 황용수, 김태완, 백충헌, 조성운, 김홍석, & 최병수. (2022). 결함허용 양자컴퓨팅 시스템 기술 연구개발 동향. [ETRI] 전자통신동향분석, 37(2).
[5] 임세진, 김현지, 김덕영, 장경배, 양유진, 오유진, & 서화정. (2023). 양자컴퓨터 플랫폼 동향. 정보보호학회지, 33(2), 31-37.
[6] IBM Quantum Computing | Qiskit Runtime, https://www.ibm.com/quantum/qiskit-runtime
[7] Introduction to Cirq | Google Quantum AI, https://quantumai.google/cirq/start/intro
[8] Steiger, D. S., Häner, T., & Troyer, M. (2018). ProjectQ: an open source software framework for quantum computing. Quantum, 2, 49.
[9] Cloud Quantum Computing Service – Amazon Braket – AWS,

https://aws.amazon.com/braket
[10] Azure Quantum – Quantum Cloud Computing Service | Microsoft Azure, https://azure.microsoft.com/en-us/products/quantum
[11] Wu, X. C., Khalate, P., Schmitz, A., Premaratne, S., Rasch, K., Daraeizadeh, S., ... & Matsuura, A. (2023). Intel Quantum SDK Version 1.0: Extended C++ Compiler, Runtime and Quantum Hardware Simulators for Hybrid Quantum-Classical Applications. Bulletin of the American Physical Society.
[12] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303-332.
[13] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 353-367). IEEE.
[14] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals-dilithium: A latticebased digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 238-268.
[15] Fouque, P. A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., ... & Zhang, Z. (2018). Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Submission to the NIST's post-quantum cryptography standardization process, 36(5), 1-75.
[16] Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., & Schwabe, P. (2019, November). The SPHINCS+ signature framework. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security(pp. 2129-2146).

※ 출처: TTA 저널 제210호