Headline

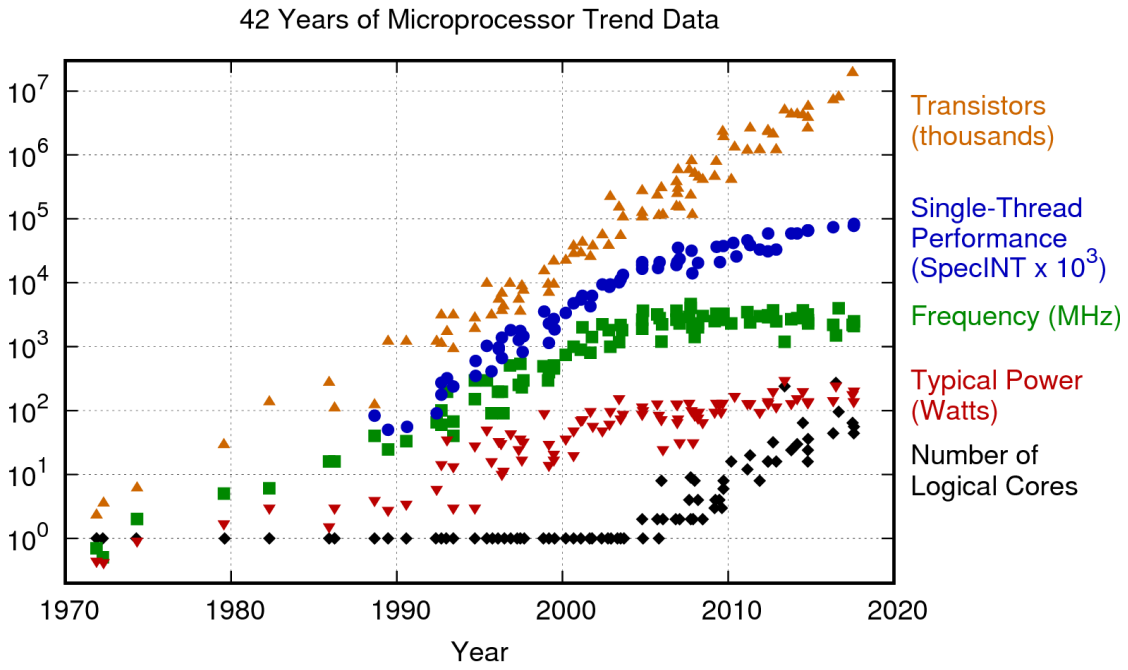
양자 컴퓨팅 기술의 발전에 따른 보안 위협과 대응 플랜

EQST/SI 솔루션사업그룹/EQST 금융사업팀 유영택 수석

■ 개요

1936 년, 앨런 튜링(Alan Turing)은 그의 논문 "On Computable Numbers, with an Application to the Entscheidungsproblem"에서 튜링 머신을 소개하며 수학적 문제를 기계적으로 해결할 수 있는 방안을 제시했다. 이와 같은 컴퓨터 과학의 기초가 되는 이론 모델을 기반으로 최초의 범용 전자식 컴퓨터 ENIAC(Electronic Numerical Integrator and Computer)가 1945 년에 탄생했다. 수천 개의 진공관을 사용해 미국 군의 수학적 계산을 빠르게 수행할 수 있었다.

이후 1947 년에 작은 크기, 낮은 전력 소모, 높은 내구성의 장점을 가진 트랜지스터가 발명되며 진공관을 대체하게 됐다. 트랜지스터가 집적회로(IC)의 기초가 되면서 컴퓨터의 성능이 급격히 향상되었고, 오늘날의 엄청난 성능 발전에 이르렀다.

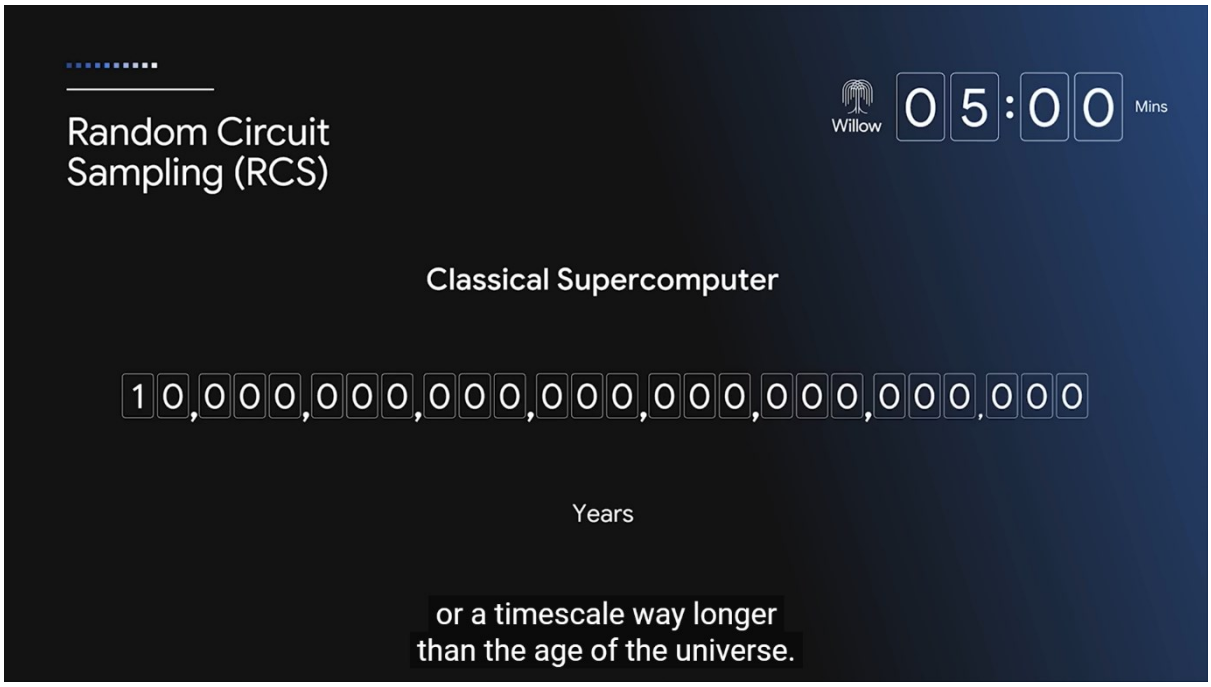


* 출처: https://www.karlrupp.net/wp-content/uploads/2018/02/42-years-processor-trend.png

그림 1. 42 Years of Microprocessor Trend Data

하드웨어의 발전에 힘입어, 최근 몇년간 Cloud 와 Deep Learning 을 기반으로 하는 AI 는 인류 문명의 가장 큰 혁신을 이끌고 있다. 하지만 지금의 컴퓨터는 트랜지스터의 집적도와 성능의 한계에 도달하고 있고 미세 공정에서의 기술적 제약, 전력 소비와 발열 문제, 병렬 처리의 한계 등 다양한 기술적 도전에 직면해 있다. 인류는 이 문제를 극복할 방법 중 하나로 '양자 컴퓨터 개발'이라는 또 다른 거대한 혁신의 문 앞에 서 있다.

2024 년 12 월 10 일 구글 퀀텀 AI(Goole Quantum AI) 연구소는 양자 칩 윌로우(Quantum Chip Willow)를 소개하며, 현존하는 가장 빠른 슈퍼컴퓨터도 10 자(秭)[1]년이 걸리는 RCS(Random Circuit Sampling) 벤치마크 계산을 윌로우(Willow)는 5 분 이내에 수행한다고 발표했다.



* 출처: https://www.youtube.com/watch?v=W7ppd_RY-UE&ab_channel=GoogleQuantumAI

그림 2. Willow Chip's RCS benchmark

아직 완전히 상용화된 양자 컴퓨터는 개발되지 않았지만[2] 현재 많은 진전을 이루고 있다. 때문에 양자 컴퓨터 개발로 인해 생길 보안 위협에 대한 이슈가 최근 전 세계적으로 대두되고 있다.

[1] 10^25, 10 의 25 승

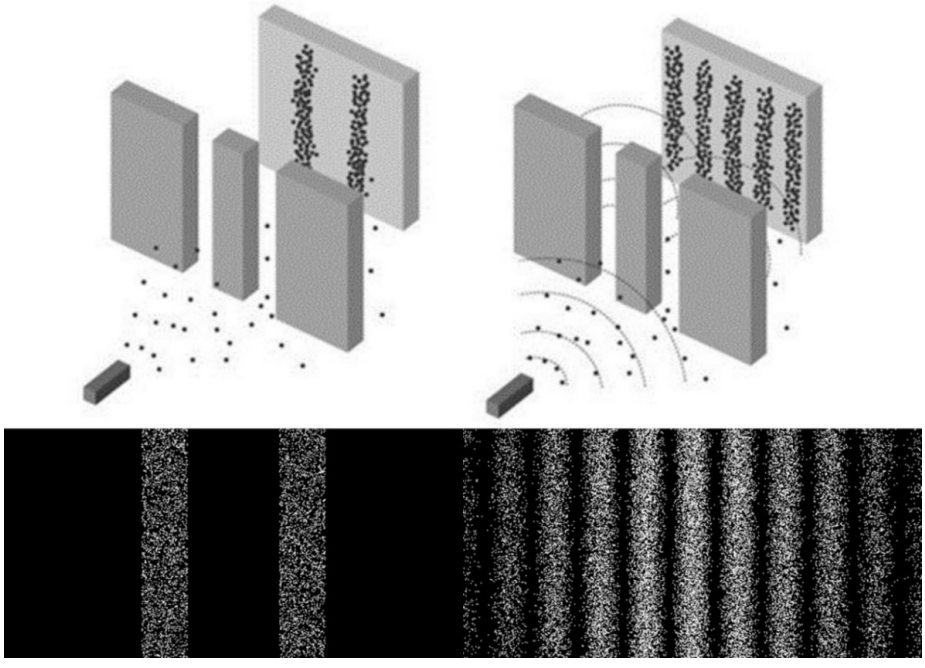
[2] 연구목적으로 상용화된 양자 컴퓨팅 서비스는 제공되고 있음

■ 양자 컴퓨터란 무엇인가?

1981 년 미국의 이론물리학자 리처드 파인만(Richard Feynman)은 고전적인 컴퓨터는 자연의 법칙을 정확하게 모델링하는데 한계가 있다고 주장했다. 자연은 양자 역학의 법칙을 따르므로, 자연과 동일한 방식으로 동작하는 양자 컴퓨터를 만들어야 한다고 말했다. 고전적인 컴퓨터는 전류가 흐르는 ON 상태, 전류가 부족하거나 없는 OFF 상태를 제어해, 이진 데이터 0 과 1 을 처리한다. 그래서 항상 0 과 1 두가지 상태 중의 하나인 비트(bit)를 기본 단위로 한다. 반면 양자 컴퓨터는 양자 역학의 기본원리인 양자 중첩(Quantum Superposition)과 양자 얽힘(Quantum Entanglement)을 이용한 양자 비트(Qubit)를 사용한다.

- 양자 중첩(Quantum Superposition)

양자 중첩은 양자가 동시에 여러 상태를 동시에 가질 수 있는 특징이다. 고전 물리학(거시 세계)에서는 한 물체의 위치가 여러 곳에 동시에 존재할 수 없고 한가지 상태만을 가진다. 하지만 미시 세계에서는 하나의 양자에 여러 상태가 확률적으로 동시에 존재하고, 측정을 하기 전에는 정확한 상태를 알 수 없다. 측정을 할 때 그 상태가 정해진다는 것이다. 이러한 현상은 양자 중첩에 대한 사고를 시작하게 된 계기인 "전자의 이중 슬릿 실험(Double-slit experiment)"에서 관찰할 수 있다.



(좌) 관측을 한 경우 **(우) 관측을 하지 않은 경우**

* 출처: https://m.blog.naver.com/iotsensor/222929618559, wikimedia

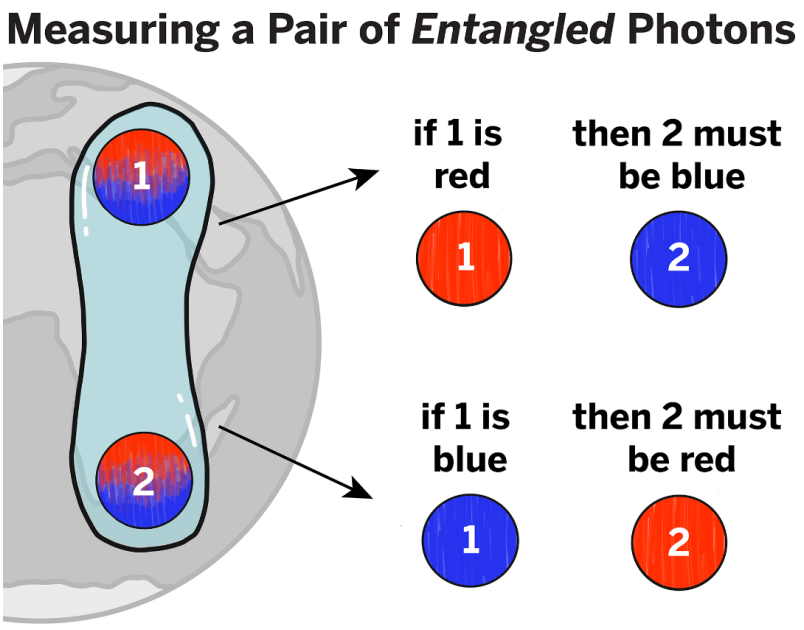
그림 3. Double-slit experiment

전자를 이중 슬릿에 무작위로 하나씩 쏘면, 관측을 할 때는 왼쪽처럼 두개의 슬릿 그대로 두개의 줄만 스크린에 나타난다. 우리가 쉽게 이해할 수 있는 결과다. 하지만 관측을 하지 않으면 오른쪽처럼 물이나 빛의 파동같이 간섭무늬가 나타난다.

이와 같은 결과가 나오는 것은 빛이나 물결의 파동처럼 전자가 두 슬릿을 동시에 통과했다는 의미이고, 하나의 전자가 두 곳에 동시에 존재한다는 뜻이 된다. 결론적으로 하나의 전자는 확률적으로 존재할 수 있는 모든 곳에 동시에 있다는 뜻이 된다. 이것이 양자 중첩이다.

- 양자 얽힘(quantum entanglement)

측정되지 않은(양자 중첩 상태) 두 입자가 공간적으로 멀리 떨어져 있을 때, 한 입자의 양자 상태가 측정이 돼 상태가 결정되면 다른 입자의 상태 또한 동시에 결정이 되는 현상을 말한다. 두 입자가 양자 얽힘 상태에 있다면 아무리 먼 거리에 있다고 하더라도, 한 입자의 스핀(Spin) 상태가 업(Up)으로 정해지면 다른 입자의 스핀(Spin)상태는 다운(Down)으로 결정이 된다. 자연에서도 가끔 광자 한 쌍이 동시에 생성되는 경우가 있는데, 두 광자는 편극 방향[3]이 수평-수직으로 서로 다른 얽힌 상태에 있다. 편극 방향이 수직이거나 수평인 중첩 상태에 있는 두 광자는 측정을 통해 한 광자의 편극 방향이 수평으로 정해지면, 다른 광자는 그 즉시 편극 방향이 수직으로 정해진다.

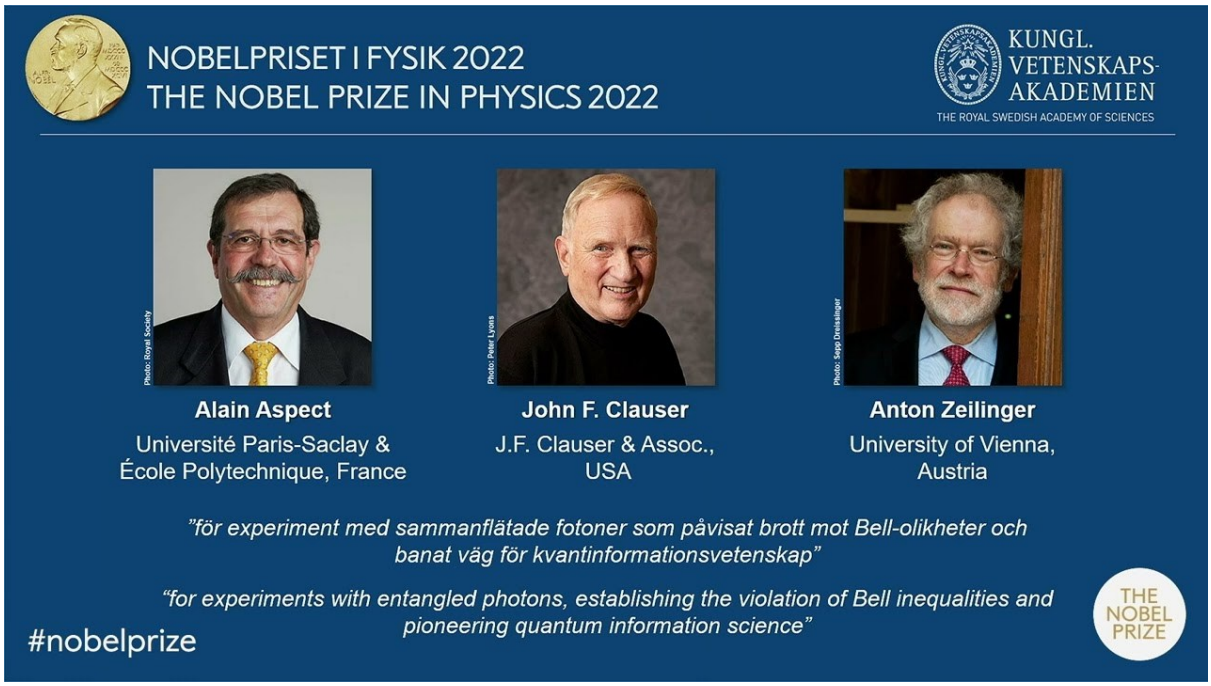


* 출처: https://quantumatlas.umd.edu/entry/entanglement/

그림 4. 양자 중첩

[3] 편극 방향: 빛은 전자기파 중 하나인데, 전기장이 공간에 퍼져 나가는 파동이다. 이 때 전기장 파동의 진동방향을 편극 방향이라고 한다.

알랑 아스페(Alain Aspect), 존 클라우저(John Clauser), 안톤 차일링거(Anton Zeilinger)는 양자 얽힘 현상을 검증하고 양자기술 시대를 여는데 공헌한 점을 인정받아, 2022년 노벨 물리학상을 수상했다.



* 출처: https://www.nobelprize.org/prizes/physics/2022/prize-announcement/

그림 5. Alain Aspect (왼쪽), John F. Clauser (가운데), and Anton Zeilinger (오른쪽)

이러한 양자 중첩과 양자 얽힘의 특성을 가진 양자 비트(Qubit)는 0과 1이 동시에 존재하는 중첩 상태로, 두 상태를 동시에 병렬적으로 계산할 수 있다. 양자 컴퓨터가 3개의 양자 비트를 사용한다고 하면, 동시에 2의3승=8개의 상태를 동시에 계산할 수 있다. 반면, 고전적인 컴퓨터가 같은 계산을 하려면 8번 연산을 해야 한다. 또한 양자 얽힘으로 두 개 이상의 양자 비트가 연결되면, 한 비트의 상태를 측정했을 때 즉시 다른 비트의 상태도 결정된다. 이로 인해 병렬 처리가 가능해지고 양자 알고리즘[4]의 성능이 비약적으로 향상된다.

[4] 양자 알고리즘: 양자 컴퓨터의 큐비트와 *양자 게이트를 활용하여 문제를 해결하기 위한 계산 방법(*양자 게이트: 고전 컴퓨터에서의 논리 게이트(AND, OR, NOT)처럼 양자 비트를 변환시키는 연산을 수행)

■ 양자 컴퓨터의 영향

양자 컴퓨터가 개발된다고 해서 모든 문제를 고전적인 컴퓨터보다 빠르게 처리하지는 않는다. 우리가 많이 쓰는 워드나 스프레드시트의 계산, 정렬 알고리즘 등 병렬성을 활용하지 않는 문제는 고전적인 컴퓨터보다 못할 수도 있다. 그렇다면 어떤 분야에 혁신을 가져오게 될 것인가?

1. 암호학의 변화

현재 대부분의 암호화 기술은 대수학적 문제에 의존하고 있다. 그러나 양자 컴퓨터는 이러한 문제를 매우 빠르게 해결할 수 있어, 현재의 암호화 기술이 무력화될 수 있다. 현재 인터넷 뱅킹·전자상거래·전자서명·인증 등 다양하게 사용되고 있는 공개키 암호화 방식은 큰 수의 소인수 분해 문제에 대한 어려움을 이용한 암호화 알고리즘이다. 대표적인 공개키 암호화 방식으로는 RSA, 디피-헬만(Diffie-Hellman) 키 교환, 타원 곡선 암호화 ECC(Elliptic Curve Cryptography)가 있다.

양자 알고리즘인 쇼어 알고리즘(Shor's Algorithm)을 사용하면 고전적인 방법으로 수십년이 걸릴 소인수 분해가 수초 내에 완료될 수 있어 은행 거래·비밀 통신·개인 정보 보호 등 다양한 분야에서 보안 위험을 초래할 수 있다. 대칭키 암호화도 그로버(Grover)의 알고리즘을 사용하면 고전적인 컴퓨터보다 제곱근만큼 빠르게 키를 찾을 수 있다. 예를 들어 n 비트의 대칭 키 암호화 방식에서는 고전적인 컴퓨터로 2^n 번의 시도가 필요하지만, Grover의 알고리즘을 이용하면 2^(n/2) 번의 시도로 키를 찾아 낼 수 있다. 암호화 키 길이가 반으로 줄어든 효과가 있는 것이다.

2. 약물 개발과 의학의 혁명

고전적인 컴퓨터는 분자의 상호작용을 정확하게 모델링하는데 한계가 있지만, 양자 컴퓨터는 분자의 구조와 화학 반응을 정밀하게 모델링해 신약 개발 과정을 빠르게 가속시킬 수 있다. 또한 개인별 유전자 분석을 통해 정교화된 맞춤 의료 서비스를 제공할 수 있게 한다.

3. 최적화 문제 해결

양자 컴퓨터는 최적화 문제를 해결하는데 뛰어나다. 물류·금융·자동차 설계·교통 관리 등에서 복잡한 최적화 문제를 효율적으로 해결할 수 있다. 예를 들면 교통 흐름을 실시간으로 최적화해 교통 혼잡을 줄이고, 도시 내에 효율적인 교통망 구축을 가능하게 한다. 기업과 산업에서는 물류와 공급망의 최적화가 가능해져 비용을 절감하고 시간 효율성을 높일 수 있다.

4. 인공지능의 발전

양자 컴퓨터는 AI의 성능을 극대화할 것으로 기대되고 있다. 기계 학습(Machine Learning)과 딥 러닝(Deep Learning) 모델은 데이터에서 최적의 파라미터를 찾는 것이 중요한다. 이를 위해 사용하는 경사 하강법(Gradient Descent)과 같은 최적화 알고리즘들은 많은 계산을 요구하고, 복잡한 데이터들은 시간이 오래 걸린다. 양자 어닐링(Quantum Annealing)과 양자 변분 알고리즘(Quantum

Variational Algorithms) 같은 양자 최적화 알고리즘을 사용하면 최적의 파라미터를 빠르게 찾을 수 있다. 또한 AI 모델은 학습과 검증을 위해 대규모 데이터 세트를 처리해야 해야 하는데, 양자 병렬 처리를 통해 데이터를 빠르게 처리할 수 있다. 이외에도 CNN(Convolutional neural network) 같은 딥러닝 구조에서 이루어지는 행렬 곱셈 연산을 훨씬 빠르게 처리할 수 있어, 딥 러닝의 학습 속도를 비약적으로 향상시킬 수 있다.

■ 양자 내성 암호화 PQC(Post-Quantum Cryptography)

고전적인 알고리즘에서는 소인수 분해에 지수 시간이 소요되지만, 1994년 피터 쇼어(Peter Shor)는 양자 중첩과 양자 푸리에 변환(Quantum Fourier Transform)을 활용해 소인수 분해를 다항 시간(polynomial time)내에 해결할 수 있는 양자 알고리즘을 개발했다. 따라서 양자 컴퓨터 환경에서는 기존의 공개키 암호화가 해독될 위협이 있는데, 이에 대응하는 새로운 공개키 암호화를 양자 내성 암호 PQC(Post-Quantum Cryptography)라고 한다.

알고리즘	설명	종류
Lattice-based Algorithms 격자 기반 알고리즘	- 격자 기반 암호화는 격자 이론(Lattice Theory)을 기반으로 수학적 격자 구조에서 나온 문제를 해결하는 알고리즘 - 현재 PQC 후보에서 가장 많이 사용	Kyber NTRU Dilithium FALCON
Code-based Cryptography 코드 기반 암호화	- 오류 정정 코드(Error-correcting codes)를 기반으로 한 암호화 기술 - 오류 정정 코드는 전송 중 발생하는 오류를 수정하기 위한 수학적 알고리즘으로, 이 원리를 암호화에 적용해 데이터를 보호하는 방식 - 이 기술의 보안성은 코드 이론에 기초하며, 문법적으로 올바르지 않은 메시지 복호화의 어려움을 기반으로 함	McEliece Niederreiter
Multivariate Quadratic Polynomials 다변수 이차 다항식 암호화	- 다변수 이차 다항식은 여러 개의 변수에 대해 이차 항(quadratic terms)과 선형 항(linear term)이 포함된 다항식 - 이와 같은 다변수 이차 방정식의 해를 찾는 문제(Multivariate Quadratic Equations)를 이용한 암호화 알고리즘	Rainbow SFLASH
Hash-based Signatures 해시 기반 서명 알고리즘	- 해시 함수를 이용하는 방식으로, 두 개의 서로 다른 메시지가 동일한 해시값을 가질 확률은 매우 낮은 충돌 저항성(collision resistance)을 활용한 알고리즘 - 양자 컴퓨터의 위협에 대해 안전한 서명을 제공	XMSS SPHINCS+
Isogeny-based Cryptography 이스오제니 암호화	- Isogeny는 타원 곡선 사이의 함수로, 한 타원 곡선의 점들을 다른 타원 곡선의 점으로 대응시키는 방식 - 순서(Order)가 같은 두 타원곡선 사이에 존재하는 아이소제니(Isogeny)를 구하는 문제의 어려움에 기반을 두는 알고리즘	SIDH SIKE

표 1. 양자 내성 암호화 알고리즘

세계 각국의 보안 기관과 학계에서는 양자 컴퓨터가 등장하기 전에 양자 내성 암호화 시스템을 개발하고 표준화하려는 노력을 기울이고 있다. 2016년 미국의 국가표준기술연구소 NIST에서는 전 세계 암호학자들에게 양자 컴퓨터의 공격에 저항할 수 있는 암호화 방법을 고안하도록 요청했고, 지원 후보들 중 가장 적절한 알고리즘을 선정해 표준화하겠다는 양자 내성 암호화 표준화 프로젝트(post-quantum cryptography standardization project)를 시작했다. 총 4 차례에 걸쳐 후보 알고리즘을 공모 받았고, 2022년 5월에 4개의 표준화 알고리즘 후보를 발표했다.

알고리즘	개발 기관(여러기관 합작)	기반 문제	용도
CRYSTALS-KYBER	CRYSTALS Team Peter Schwabe, MPI-SP & Radboud University 외 10명 https://pq-crystals.org/	격자 기반	공개키 암호화키교환
CRYSTALS-Dilithium	CRYSTALS Team Vadim Lyubashevsky, IBM Research Zurich 외 7명 https://pq-crystals.org/	격자 기반	전자서명
FALCON	Thomas Prest, PQShield 외 9명 https://falcon-sign.info/	격자 기반	전자서명
SPHINCS+	SPHINCS+ Team Andreas Hülsing, Eindhoven University of Technology & SandboxAQ 외 17명 https://sphincs.org/	해시 기반	전자서명

표 2. 2022 년 NIST 선정 PQC 알고리즘

공개키 암호화 PKE(Public-Key Encryption)와 키교환 알고리즘 KEMs(Key Encapsulation Mechanisms)으로 CRYSTALS-KYBER를 선정했고, 전자서명(digital signatures) 알고리즘으로 CRYSTALS-Dilithium을 선정했다. 추가로 디지털 서명 알고리즘으로 FALCON 과 SPHINCS+도 표준화될 계획이다.

국내에서도 양자 내성 암호화가 연구 개발 중이고, 아래 4개의 알고리즘이 개발되어 2017년에 NIST 공모에 제출됐다. 이 중 HimQ와 Lizard 알고리즘은 한국정보통신기술협회(TTA)의 표준문서로 등록됐다.

알고리즘	개발기관	기반 문제	용도
EMBLEM and R.EMBLEM	고려대학교	격자 기반	공개키 암호화
pqsigRM	양자내성암호연구단 kpqc	코드 기반	전자서명
HimQ	국가수리과학연구소	다변수 이차 다항식	전자서명
Lizard	서울대학교 KISA(한국인터넷진흥원)	격자 기반	키교환

표 3. 국내 개발 양자 내성 알고리즘

■ 양자 내성 암호화 PQC 적용 분야

양자 내성 암호화는 암호화가 사용되는 분야, 특히 공개키 암호화가 사용되는 분야에 모두 적용이 된다. 공개키 암호화를 사용하는 부분은 양자 내성 암호화를 사용해야 하고, 대칭키를 사용하는 부분은 AES 256bit 이상의 키를 사용해야 한다. SHA2, SHA3 또한 256bit 이상의 키를 사용해야 한다(기술의 발전, 취약점 발견에 따라 대칭키 보안 기준도 계속 변경될 것이다).

TLS(HTTPS)

대표적으로 인터넷에 사용되는 TLS(HTTPS) 프로토콜의 경우, 양자 내성 암호화 적용이 필수다. 양자 내성 암호화를 사용해 키교환을 한 후, 교환된 패킷 암호 대칭키는 256bit 이상을 사용해야 한다.

클라이언트	서버	
브라우저	웹서버	WAS
PQC 키교환 적용	PQC 키교환 적용	웹서버<->WAS 간 데이터 보호로 공개키 암호화가 필요할 경우 PQC 키교환 적용 필요

표 4. TLS PQC 전환

VPN(Virtual Private Network)

VPN은 공개키 방식으로 대칭키를 교환하고, 해당 대칭키로 암호화된 터널을 만들어 안전하게 통신을 한다. TLS와 마찬가지로 키교환에 사용되는 공개키 암호화 방식은 PQC로 전환되어야 하고, 교환된 대칭키는 256bit 이상이어야 한다.

미들박스(Middlebox)

미들박스는 네트워크 장치나 시스템에서 패킷을 필터링 변경, 조작하는 네트워크 장비를 말한다. 주요 장비로는 방화벽(Firewall), NAT(Network Address Translation), 로드 밸런서(Load Balancer), IDS/IPS(Intrusion Detection/Prevention System)이 있다.

양자 내성 암호화는 주로 애플리케이션 계층(Layer 7)에 속하고, 미들박스의 동작은 주로 네트워크 계층(Layer 3), 전송 계층(Layer 4) 속한다. 따라서 미들박스는 암호화된 데이터를 전달하거나 검사하는 역할을 하기 때문에 양자 내성 암호화가 도입된 후에도 그 동작에는 큰 변화가 없을 수 있다.

하지만 다음과 같은 기능은 미들박스에도 PQC가 적용되어야 사용할 수 있다.

TLS/SSL 검사 및 종료: 암호화된 트래픽을 복호화해 내부 네트워크에 전달

암호화 검사: 암호화된 트래픽을 복호화해 검사하는 기능

사물인터넷(IoT)

IoT 네트워크는 수많은 장치들이 상호작용하는 환경이고, 안전한 통신을 위해 공개키 방식으로 키를 교환 후 대칭키로 암호화해 통신하는 것이 일반적이다. 따라서 키교환 방식을 PQC로 전환을 해야 하지만 IoT 장치는 자원제한이 있기 때문에, 실제 PQC를 구현하는데 어려움이 있을 수 있다. 저전력 IoT 장치의 경우에는 연산 비용이 낮고, 메모리와 대역폭의 요구사항이 적은 경량 양자 내성 암호화(Lightweight Post-Quantum Cryptography, Lightweight PQC) 적용이 필요하다.

금융거래/클라우드(Cloud) 환경

모바일 금융거래, 클라우드 환경의 경우 앞서 말한 TLS, VPN, 미들박스의 내용을 모두 포함하고 있다. 거기에 추가로 사용자 인증, 전자 서명이 중요하다.

모바일 금융 서비스의 경우, 거래를 하거나 사용자 인증이 필요하다면 전자 서명으로 금융인증서, 공동인증서와 같은 공개키 암호화 방식을 사용한다. 따라서 PQC 방식의 금융인증서, 공동인증서의 적용이 필요하다.

클라우드 서비스의 경우도 사용자 인증, 접근 제어에 있어 공개키 방식의 전자 서명이 사용되기 때문에 PQC 방식의 전자 서명이 필요하다. 또한 클라우드에서 데이터를 저장할 때 사용하는 대칭키 암호화는 공개키 암호화로 키 관리를 하기 때문에, 이 또한 PQC를 적용해 안전하게 키를 관리해야 한다.

블록체인/비트코인

블록체인은 거래의 무결성을 확인하기 위해 공개키 암호화 방식뿐 아니라 해시 방식을 같이 사용하고 있다. 해시 방식은 SHA-256이기 때문에 양자 컴퓨터의 공격으로부터 안전하다고 볼 수 있다.

그러나 비트코인의 전자 지갑은 그렇지 않다. 비트코인은 ECDSA(타원 곡선 암호)라는 공개키 암호화 방식을 사용하는데, 비트코인 초기에는 공개키가 지갑의 주소로 사용되는 p2pk(Pay-to-PubKey) 방식을 사용했다. 따라서 양자 컴퓨터는 이 공개키로 개인키를 알아 낼 수 있었다. 2010년 이후로는 사용자의 공개키가 SHA-256 해시와 RIPEMD-160 해시로 변환돼 주소로 사용되는 P2PKH(Pay-to-PubKey-Hash) 방식을 사용하기 때문에, 지갑 주소만으로 개인키를 알아 낼 수 없게 됐다. 하지만 거래가 이루어지면 상대방에게 공개키가 드러나게 되기 때문에 양자 컴퓨터의 공격에 여전히 취약하다. 따라서 ECDSA(타원 곡선 암호) 알고리즘을 PQC로 전환하는 것이 필요하다.

업데이트/패치 무결성 검증

펌웨어, 시스템 업데이트, 패치처럼 중요한 파일들은 그 변조 여부를 확인하기 위해 전자 서명이 되어 있다. 개인키로 파일에 서명이 되고, 공개키로 검증을 함으로써 무결성을 확인한다. 양자 컴퓨터가 개발되면, 공개키로부터 개인키를 알아내 업데이트 파일에 악성코드를 심고 다시 서명하는 방식으로 무결성 검증을 우회할 수 있다. 따라서 PQC가 적용된 전자 서명을 사용해야 한다. 최근 공급망 공격(Supply Chain Attack)[5] 사례가 늘고 있는 만큼 업데이트/패치 파일의 무결성 검증이 중요해지고 있다. 때문에 필수적으로 PQC 적용이 필요한 분야다.

■ 양자 컴퓨터의 현주소

양자 컴퓨터가 얼마나 발전해야 현재 사용하는 암호화에 위협이 될까? 공개키 암호화로 양자 컴퓨터 공격이 가능하려면 수천개의 큐비트가 필요하다고 한다.

공개키 암호화 알고리즘	공격에 필요한 큐비트 수
RSA-1024	약 2,000개
RSA-2048	약 4,000~5,000개
RSA-3072	약 7,000개 이상
ECC-256	약 2,000 ~ 2,500개
ECC-512	약 4,000개

* 출처: "Quantum Computing for Computer Scientists" (Noson S. Yanofsky and Mirco A. Mannucci

표 5. 현재 공개키 암호 시스템 공격에 필요한 큐비트 수

양자 컴퓨터 개발에 가장 앞서 나가는 기업은 IBM과 Google로 큐비트 수가 100개 정도다.

기업	기반 기술	큐비트 수	기타
IBM Quantum	초전도(Superconducting)	127 (Eagle)	https://www.ibm.com/quantum
GoogleQuantumAI	초전도(Superconducting)	105 (willow)	https://quantumai.google
IonQ	이온트랩(Ion Trap)	35	https://ionq.com
Microsoft Azure Quantum	토폴로지 큐비트 (Topological Qubit)	개발 중	https://quantum.microsoft.com
D-Wave	양자 어닐링 (Quantum Annealing)	5000[6]	https://www.dwavesys.com

표 6. 기업별 양자 컴퓨터 개발

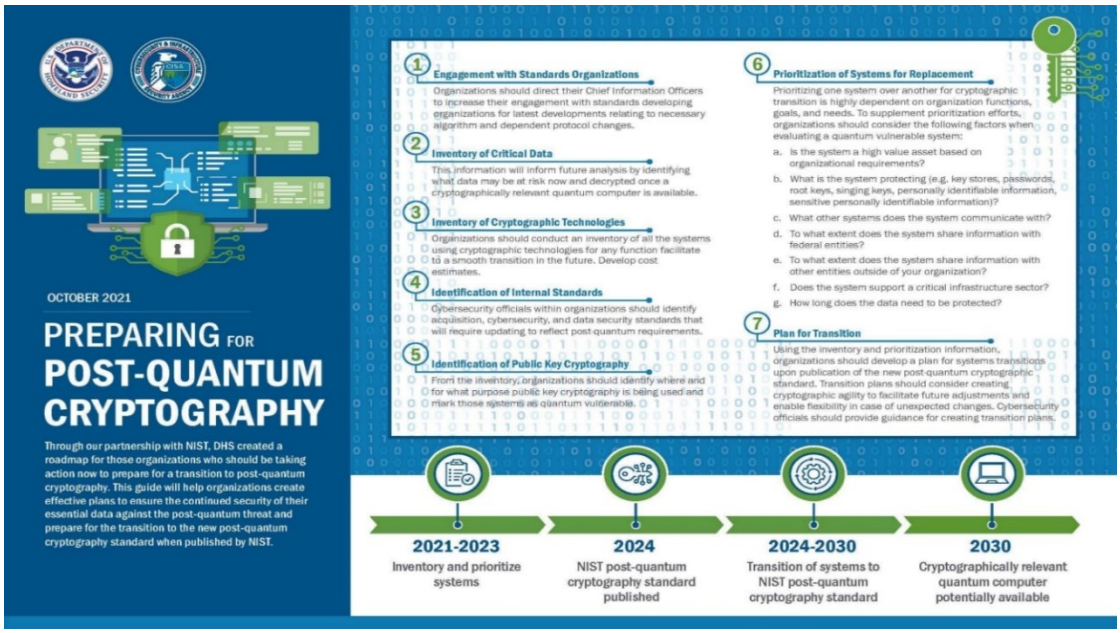
[5] 공격자가 기업이나 조직의 공급망에 침투하여 악성 코드를 배포하거나 시스템을 침해하는 방식

[6] 큐비트 수가 많아 보이는 이유는 양자 어닐링의 특성과 구현 방식 때문이다. 특정 문제를 빠르게 푸는 데 특화된 양자 컴퓨터로, 다른 범용 양자 컴퓨터의 큐비트 수와 똑같이 비교할 수 없다.

양자컴퓨팅과 양자 암호 업계에서는 2030년이 되면 양자 컴퓨터가 공개키 암호화 시스템에 실질적인 위협이 될 것으로 예상하고 있다.

■ 맺음말

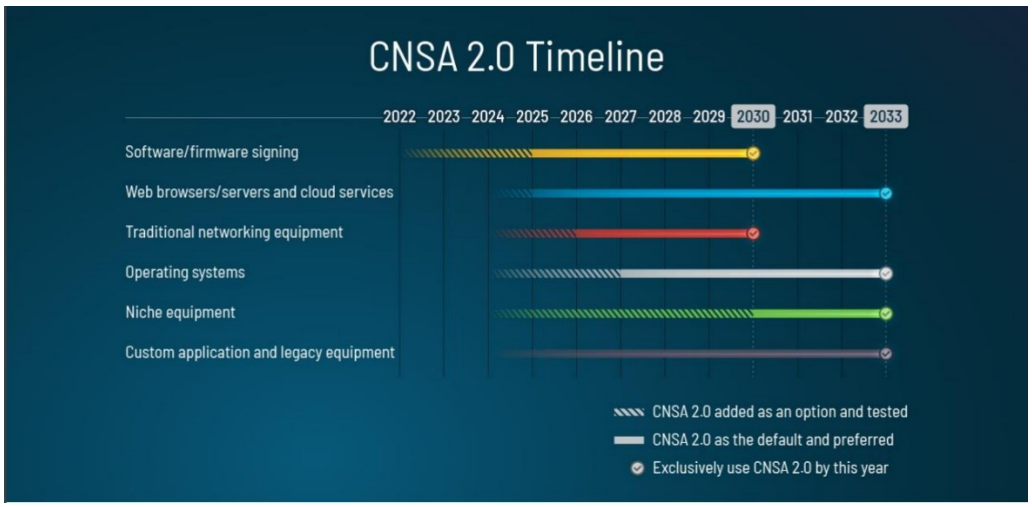
미국 정부는 2022년 5월에 PQC로 전환하는 미국 정부의 사이버 보안 전략(NSM-10)를 발표했다.



* 출처: 미국 국가안전보장회의(National Security Council, NSC)

그림 7. 미국 사이버 보안 전략 NSM-10

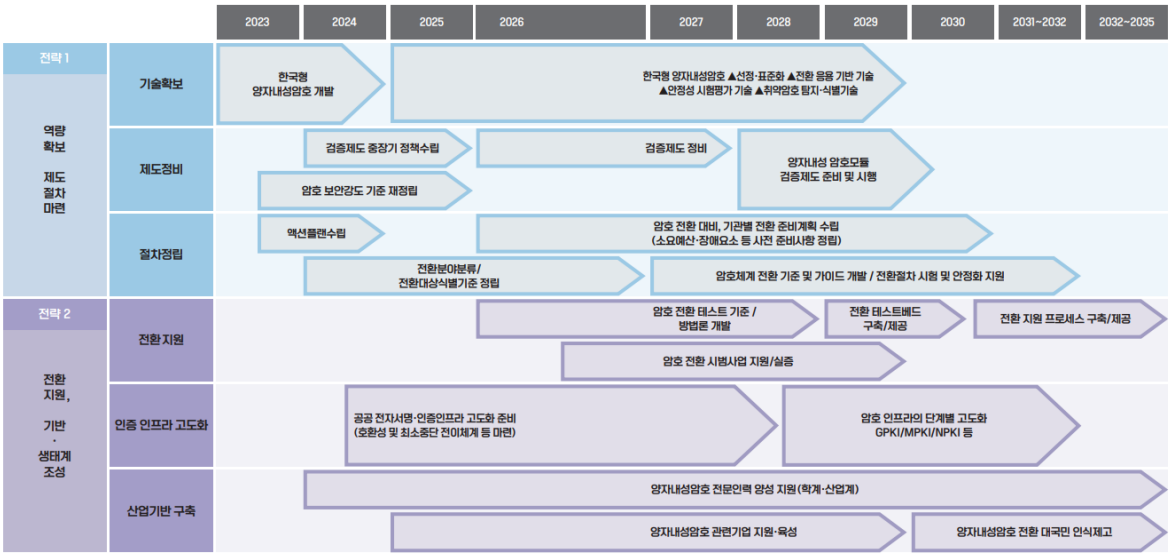
그 후 9월에는 국가안보국(NSA National Security Agency | Cybersecurity Advisory)이 2025년에 소프트웨어, 펌웨어 분야부터 양자 내성 암호를 적용하기 시작해 2033년까지 서버, 클라우드 등 모든 분야에 걸쳐 완료하는 타임라인 "CNSA (Commercial National Security Algorithm Suite) 2.0"을 공개했다.



* 출처: NSA National Security Agency

그림 8. NSA CNSA 2.0 타임라인

국내에서는 국가정보원과 과학기술정보통신부가 2035년까지 국가 암호 체계 전반을 양자 내성 암호로 전환하기 위한 "양자 내성 암호 마스터플랜"을 발표했다. 작년에 마스터플랜 분야별 실행 계획을 마련했고, 2030년까지 양자 내성 암호 체계로 전환을 위한 제도적 기반을 구축할 예정이다. 이후 2035년까지 암호 체계 전환 테스트베드와 통합지원센터를 구축 운영하는 등 관련 기술을 개발하고 필요한 정책을 지원한다는 내용이다.



* 출처: 국가정보원

그림 9. 국내 양자내성암호 마스터플랜

양자 컴퓨터는 글로벌 패권에서도 우위를 가지기 위한 전략자산으로 간주되고 있다. 각 국의 정보기관들은 양자 컴퓨터를 개발하더라도 외부에 공개하지 않고 타국의 국가기밀이나 산업 기밀을 해독하는데 활용할 것으로 예상된다. 때문에 이런 위협에 대비하기 위해서 양자 내성 암호 전환을 철저히 준비해야 한다.