

양자컴퓨터와 NIST 양자내성암호 표준화 동향

한성대학교 장경배
지도교수 서화정

Contents

양자 컴퓨터

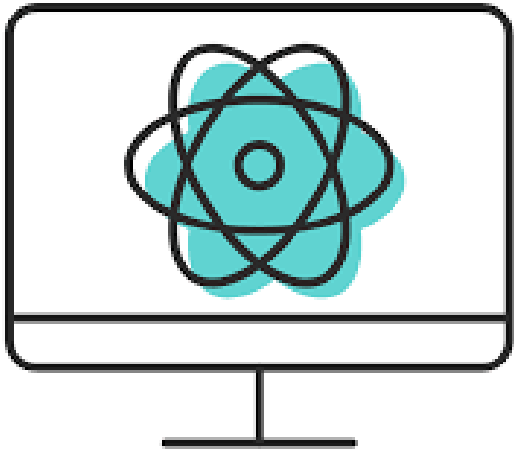
양자 알고리즘 : Shor

양자내성암호

NIST 양자내성암호 표준화 동향

결론





양자 컴퓨터란?

기존 컴퓨터가 사용하는 일반적인 비트가 아닌
양자역학적 원리를 활용한 양자비트라는 개념을
사용하는 새로운 개념의 컴퓨터

양자 컴퓨터

양자 컴퓨터가 중요한 이유

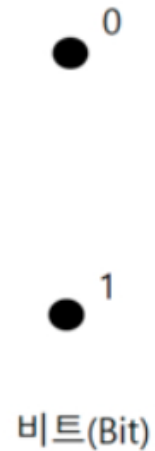
기존 컴퓨터에서 연산속도의 한계로 수행 불가능했던 문제에 대하여 뛰어난 해결능력을 가지고 있다.

양자 컴퓨터가 끼친 영향

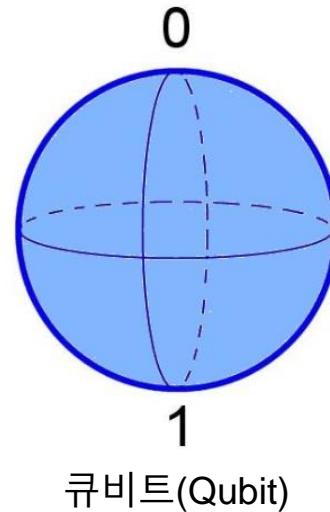
현재 사용되는 수학적 난제에 기반한 암호시스템들은 기존 컴퓨터가 풀어내기 매우 어렵다. 하지만 양자 컴퓨터가 등장한다면 빠른 시간안에 풀어낼 수 있다.

✖ 암호체계의 붕괴 ✖

양자 컴퓨터 : 큐비트(Qubit)



0과 1 둘 중 하나를
결정하여 정보를 표현



0 이 표현될 수도 있고
1 이 표현될 수도 있다.

이렇게 자신의 상태가
확률로서 존재하는 것이 바로 큐비트

➡ 중첩(Superposition)

양자 컴퓨터 : 큐비트 (Qubit)

관측

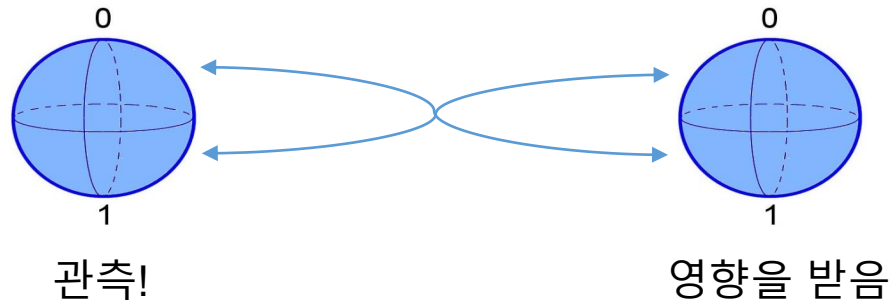
확률상태로 존재하던 큐비트의
상태를 결정하는 행위



얽힘

관측으로 인해 큐비트의 상태가 결정 되었을 때
관측된 큐비트와 얽혀 있는 다른 큐비트의 상태까지 결정되는 것

➡ 데이터가 한순간에 다른 곳으로 이동하는 것으로 보임




양자 컴퓨터 : 큐비트 (Qubit)

Bit

2bit → 00
2bit → 01
2bit → 10
2bit → 11

- 한번에 한가지 정보 표현
- 직렬처리

Qubit

2 Qubit 
00
01
10
11

- 한번에 여러가지 정보 표현
- 병렬처리
- 메모리 공간 확보
- 지수승으로 증가 (예 : 3 큐비트 -> 8가지 정보 표현 가능)

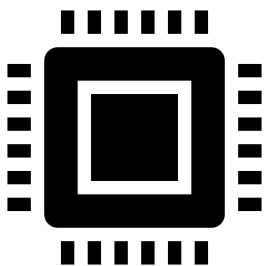
양자 컴퓨터 : 기대효과

양자컴퓨터의 핵심은 병렬성



딥 러닝(Deep learning)

인공신경망을 이용하여 컴퓨터 스스로 더 나은 결과를 도출하며 학습해 나가는 기술
병렬처리에 강한 GPU의 눈부신 발전은 딥러닝 기술의 발전 또한 가져왔다.



전사공격(Brute force attack) : 무차별 대입공격

Key 가 될 수 있는 모든 경우의 수를 시도해보는 공격 방법

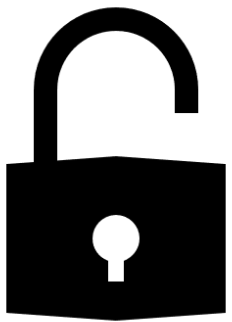
기존 컴퓨터



양자 컴퓨터



양자 알고리즘



양자 컴퓨터의 등장과 함께 나타난 새로운 양자 알고리즘

기존 컴퓨터에서 해결하기 어려운 수학적 난제들을 효율적으로 풀어냄

→ 이러한 난제에 기반한 현재 암호시스템들을 위협

양자 알고리즘 : Shor

1994년 수학자 Shor는 기존 컴퓨터에서의 난제인 **소인수분해 문제**를

효율적으로 풀어낼 수 있는 양자 알고리즘을 제안

커다란 두 소수를 곱하는 것은 쉽지만 이렇게 곱해진 매우 커다란 정수를 두 소수로 다시 분해하는 것은, 두 소수 중 하나를 모른다면 매우 어려운 일 예제) $N = pq$

$$O\left(e^{1.9(\log N)^{1/3}(\log \log N)^{2/3}}\right) \xrightarrow{\text{use Shor's Algorithm}} O\left((\log N)^2(\log \log N)(\log \log \log N)\right)$$

지수 차원의 복잡도

Before

→

다항시간내에 해결

After

결과 : 소인수 분해의 어려움에 기반한 암호시스템들을 무너뜨릴 수 있다. 예시) RSA

양자 알고리즘 : Shor

소인수 분해를 푸는 과정에서

주기 찾기 알고리즘을 이용하여 $f(x) = a^x \bmod N$ 일 때
 $f(x + r) = f(x)$ 를 만족하는 차수 r 을 구한다.



주기 찾기 문제
(Order Finding)

$$f(x) = a^x \bmod N \quad N = 15, a = 7$$

예제

$$7^1 > 7 \bmod 15 = 7$$

$$7^2 > 49 \bmod 15 = 4$$

$$7^3 > 343 \bmod 15 = 13$$

$$7^4 > 2401 \bmod 15 = 1$$

$$7^5 > 16807 \bmod 15 = 7$$

답 : $r = 4$



양자 알고리즘 : Shor

Problem

$f(x + r) = f(x)$ 를 만족하는 차수 r 을 구한다.

Solution !

양자 컴퓨터가 여러 상태에 동시에 존재할 수 있다는 성질을 이용

함수 $f(x)$ 의 주기를 계산하기 위해서 모든 x 점에서의 함수 값을 동시에 계산한다.

반복이 필요한 주기 찾기 작업을 한 번의 계산으로 가능하게 하여 계산 복잡도를 크게 낮춘다!

→ 쇼어 알고리즘을 이용하여 소인수분해 문제에 기반한 기존 암호시스템을 무너뜨린다.

양자 알고리즘

양자컴퓨터 시대에 대한 현재 암호시스템의 상황 (NIST 발표)

| 유형 | 알고리즘 | 목적 | 영향 |
|-----|----------------|---------------------------------|-----------------|
| 대칭키 | AES | Encryption | 키 길이 증가 필요 |
| | SHA-2, SHA-3 | Hash | 출력 길이 증가 필요 |
| 공개키 | RSA | Signature, Key establishment | 더 이상 안전하지 않음 |
| | ECDSA, ECDH | Signature, Key exchange | |
| | DSA | Signature, Key exchange | |
| | Diffie Hellman | Key exchange | |

양자 컴퓨터와 양자알고리즘의 영향

양자 컴퓨터 효과

- Shor 이론은 정립되었으므로 실현 가능한 양자 컴퓨터만 있으면 되는 상황
- 암호체계의 이러한 큰 변화는 현재까지 없었음, 대칭키와 해쉬는 그나마 큰 변화가 없음
- 블록체인 또한 해쉬기반과 공개키 방식이니 아예 구조적으로 개편이 필요함
- 기존 금융권에서 사용하는 공개키 -> 2048비트 공개키 사용
- 5천 큐비트 -> 4.5분에 2048 비트의 공개키를 풀 수 있음 (기존 컴퓨터 3억년)
- 이에 **IBM**은 10년안에 기존 공개키 체계 붕괴 예상

양자 내성암호(Post Quantum Cryptography)



Cryptography

양자역학의 발전과 빠르게 진화하는 양자컴퓨터에 대비하여
양자 컴퓨터의 계산능력에 내성을 가진 암호가 필요한 상황

양자내성암호(Post Quantum Cryptography)

양자 내성암호(Post Quantum Cryptography)

모든 수학적 분야에 대하여 양자컴퓨터가

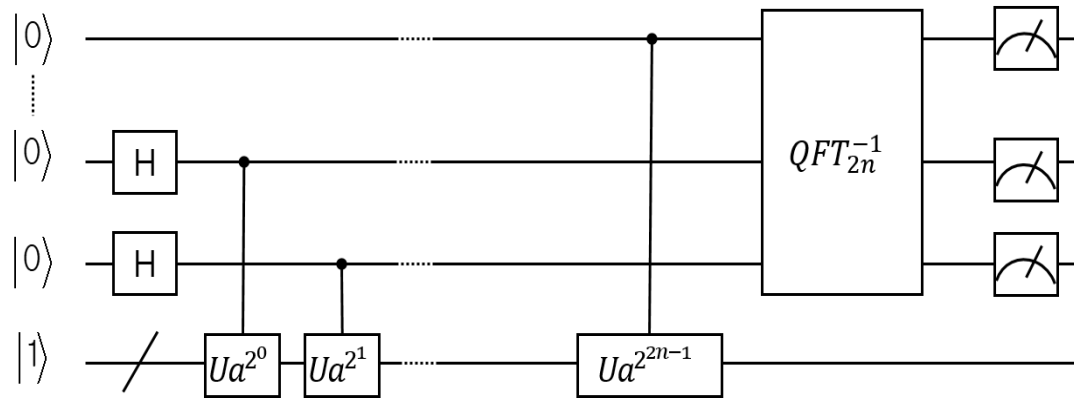
기존컴퓨터보다 빠른 것은 아니기 때문에

양자컴퓨터에 내성을 가진 새로운 수학적문제에 기반한 암호들이 주목받고 있음

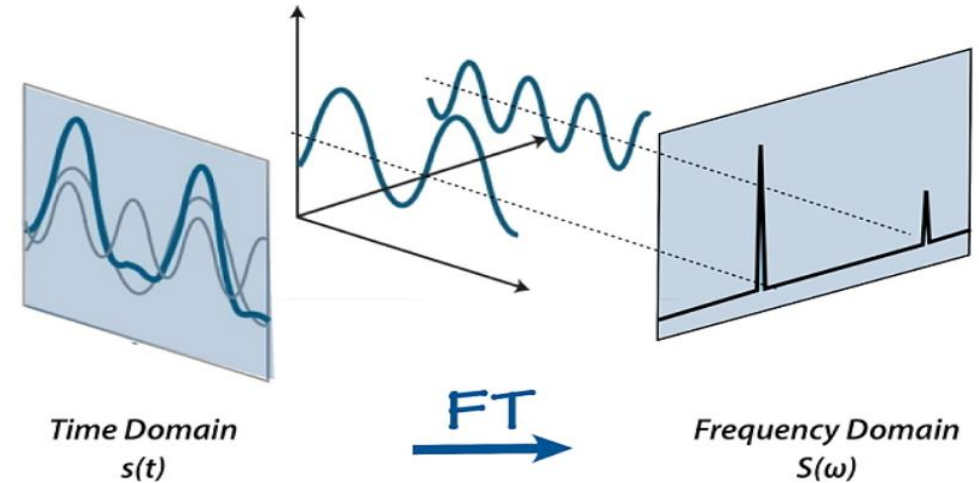
양자컴퓨터는 병렬적인 계산이 가능하기 때문에 한번에 많은 정보를 표현할 수는 있다.

하지만 정보에 계산 된 모든 값을 추출할 수는 없다.

양자 내성암호(Post Quantum Cryptography)



Shor 알고리즘 주기찾기 회로 ($f(x+r) = f(x)$)



양자 푸리에 변환

어떠한 양자 측정도 그 모든 계산 된 값을 전부 추출할 수는 없으나

함수의 출력 값의 광역적인 성질에 대해서 → **주기**

그 함수에 대한 정보를 얻어낼 수 있는 방법이 존재한다는 것

NIST 양자내성암호 표준화 동향



양자내성암호(PQC)의 필요성 대두되는 상황, NIST는

PQC 표준화 공모전을 개최, 국제적으로 많은 암호알고리즘이 참가했고

제안된 알고리즘을 검증 및 평가해가며 후보 알고리즘을 점점 추려내고 있다.

진행상황

Round 1 : 자신들의 제시한 최소수용조건을 만족하는 알고리즘

Round 2 : 효율성 및 최적화구현 제시

4

NIST 양자내성암호 표준화 동향

Round 1에서는 NIST가 제시한 성능 조건을 만족하는 69개의 양자내성암호 알고리즘이 선정

2019년 1월 30일, 표준화 단계가 Round 2로 진행됨에 따라 암호알고리즘의 안전성과 실용성에 대하여 평가, 69개에서 26개의 후보자로 좁혀졌다.

Round 2, 26개의 후보 알고리즘 표 ➡

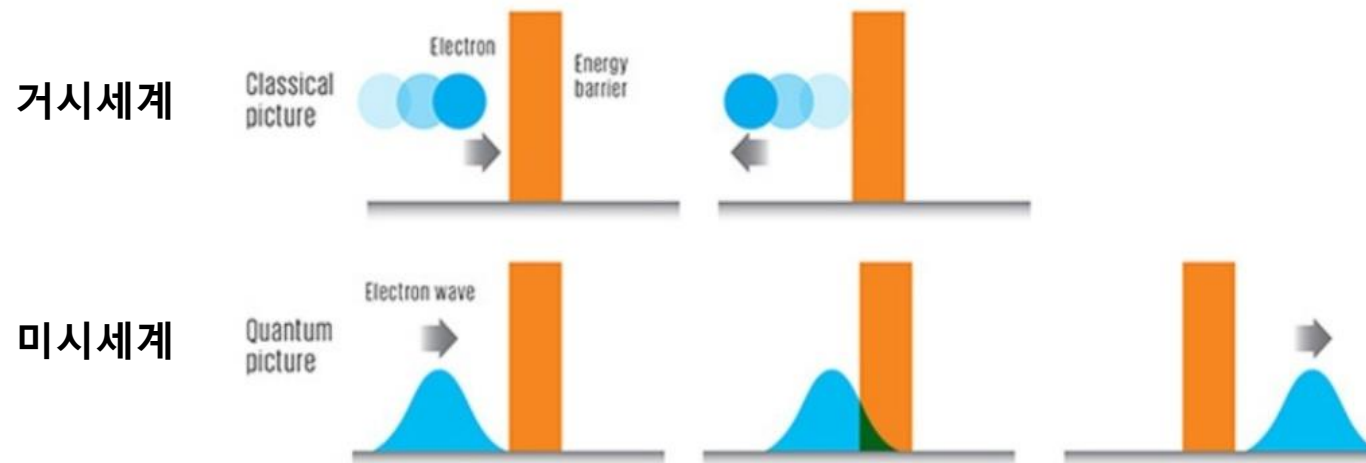
| 유형 | 공개키암호/키관리 | 서명 |
|--------|---|--|
| 격자 | CRYSTALS-KYBER Frodo LAC Newcome NTRU NTRU Prime Round 5 SABER Three Bears | CRYSTALS-DILITHIUM FALCON qTESLA |
| 부호 | BIKE Classic McEliece HQC LEDACrypt NTS-KEM ROLLO RQC | |
| 해쉬 | | SPHINCS+ |
| 다변수다항식 | | GeMSS LUOV MQDSS Rainbow |
| 아이소제니 | SIKE | |

결론

양자 컴퓨터의 영향

양자 터널링 현상으로 인한 반도체의 한계 ∞ 반도체의 눈부신 발전으로 인한 한계 (미세공정)

빠른 시뮬레이션 -> 의학, 딥러닝



결론

양자 컴퓨터의 영향

NIST 로드맵 : 2024년 PQC표준화를 완료하겠다

하지만 2020 중반에 깨질거라 예상 -> 기업들의 불만

난수성을 확보해야 하다 보니 양자내성암호의 효율성은 기존 암호 시스템보다 수 십, 수 백 배 떨어짐

새로운 암호체계를 도입하기 위해선 개발, 협의, 표준화, 안전성검증 등의 이유로 오랜 시간이 소요

현재 우리는 양자컴퓨터 시대에서도 견뎌낼 수 있는 견고한 양자내성 암호체계 구축이 시급한 상황!

Q & A

감사합니다

