Post Quantum Cryptography

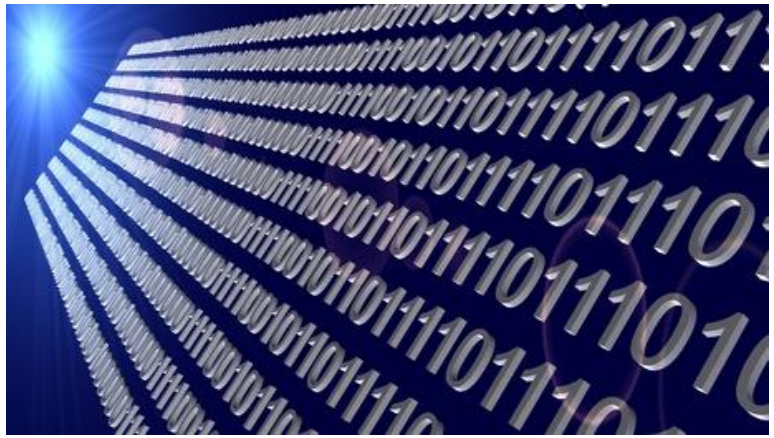
https://youtu.be/AMAsAxN19rA

한성대학교 IT응용시스템공학과 장경배

Post Quantum Cryptography (PQC) ??

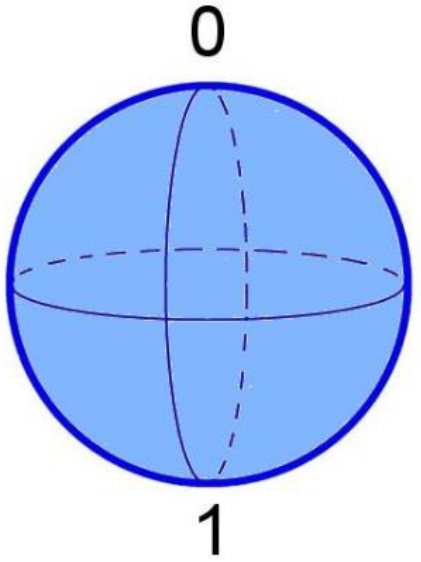
양자 컴퓨터의 계산능력에 내성을 가진 암호 시스템

양자 컴퓨터



기존 컴퓨터

0과 1 둘중 하나로 정보를 표현

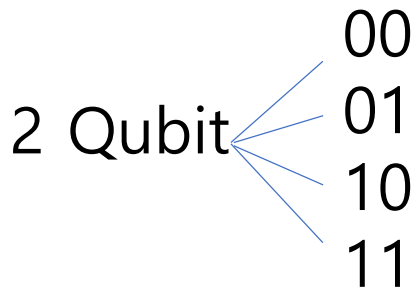


Qubit

0 1 0,1을 동시에

Qubit

2bit ➡ 00
2bit ➡ 01
2bit ➡ 10
2bit ➡ 11



한번에 한가지 정보만 처리

이러한 병렬 처리 형태로

큐비트 개수당 2의 N제곱으로 증가

2큐비트는 동시에 4가지 정보 표시 가능

양자컴퓨터 시대

IBM 50 Qubit 양자컴퓨터

현재의 과제는 연산과정에서의 오류율을 낮추는 문제

1125조8999억가지 정보를 동시에 표현 가능

PQC의 필요성

Shor는 소인수분해 문제를 빠르게 처리할 수 있는 양자 알고리즘을 제안

이러한 알고리즘이 적용가능한 양자 컴퓨터가 개발되면 기존 암호화 시스템을 깨트릴 수 있으며

현재 세계적으로 널리 쓰이고 있는 공개키 암호화 시스템인 RSA 또한 그 대상이다.

그러므로 양자컴퓨터의 계산능력에 내성을 가진 암호화 시스템이 필요하다.

주요 PQC 후보

- Lattice-Based : 격자 기반
- Code-Based : 부호 기반
- Hash-Based : 해쉬 기반
- Isogeny-Based : 아이소제니 기반
- Multivariate : 다변수 다항식 기반

격자기반 암호, Lattic-based Cryptography

상대적으로 효율적인 구현과 엄청난 간결성 뿐만 아닌
매우 강력한 안전성을 보증하며 양자 컴퓨터에 대항한 안전성까지 신뢰된다.

격자란?

주기적 구조 (주기적인 서브그룹으로 그 구조를 이루는것 ex 철도레일)
와 n차원 공간의 점들의 집합

NRTU public key cryptosystem

인수분해나 이산로그 문제에 기반하지 않은 최초의 공개키 암호화 시스템

암호화, 복호화 속도가 빠르다

RSA나 ECC를 대체할 수 있음

격자 안에서 가장 짧은 벡터를 찾는 문제에 기반하며
-> Shortest Vector Problem (SVP)

다항식 환 상에서 연산이 이루어진다..

알고리즘(Key generation , Encryption)

파라미터 (N,p,q) 설정

개인키

1. Bob은 다항Ring **R**상에서 작은 계수들을 가지는 N-1차의 **f** 그리고 **g**를 private로 가지게 된다.

2. f에대하여 f modulo q 에 대한 역과 f modulo p 에 대한 역을 계산하여 개인키 생성

$$\mathbf{f}*\mathbf{f}_q = 1 \text{ (modulo } q\text{)} \qquad \mathbf{f}*\mathbf{f}_p = 1 \text{ (modulo } p\text{)}$$

공개키

$$\mathbf{h} = p\mathbf{f}_q * \mathbf{g} \text{ (modulo } q\text{)}.$$

암호화

Alice는 자신이 보낼 메시지 **m**을 랜덤하게 선택된 다항식 **r**과 공개키 **h**를 사용하여 암호화 한다.

$$\mathbf{e} = \mathbf{r}*\mathbf{h} + \mathbf{m} \text{ (modulo } q\text{)}.$$

복호화

개인키 **f** 를 사용

f*e (modulo *q*). ➡ a

a (modulo *p*) ➡ b

fp*b (modulo *p*). ➡ 원본메세지 m을 획득

복호화 증명

$a = f * e \pmod q$

$= f * (r * h + m) \pmod q \quad \because e = r * h + m \pmod q$

$= f * (r * pf_q * g + m) \pmod q \quad \because h = pf_q * g \pmod q$

$= pr * g + f * m \pmod q$

$mod\ p$로 계수제거하여

$\rightarrow f * m \pmod p$ 획득

마지막으로 f_p를 곱셈역원 곱하여 원본메세지 m 복구 완료

암호화, 복호화 예제

파라미터

$N=11 \quad q=32 \quad p=3$

f에대하여 f modulo q 에 대한 역과 f modulo p 에 대한 역을 계산하여 개인키 생성

$f*f_q = 1 \text{ (modulo } q) \qquad f*f_p = 1 \text{ (modulo } p)$

개인키

$$\mathbf{f} = -1 + X + X^2 - X^4 + X^6 + X^9 - X^{10}$$

$$\mathbf{g} = -1 + X^2 + X^3 + X^5 - X^8 - X^{10}$$

$$f_p = 1 + 2X + 2X^3 + 2X^4 + X^5 + 2X^7 + X^8 + 2X^9$$

$$f_q = 5 + 9X + 6X^2 + 16X^3 + 4X^4 + 15X^5 + 16X^6 + 22X^7 + 20X^8 + 18X^9 + 30X^{10}$$

$x - 1$

-2 mod 3 = 1

$$-2x^{19} + x^{18} - x^{17} + 2x^{16} + x^{15} + x^{12} - x^{11} + 6x^{10} + 3x^9 - x^8 - x^7 + 4x^6 + x^5 - x^4 + 3x^2 - x - 1$$

공개키

$$\mathbf{h} = p\mathbf{f}_q*\mathbf{g} = 8 + 25X + 22X^2 + 20X^3 + 12X^4 + 24X^5 + 15X^6 + 19X^7 + 12X^8 + 19X^9 + 16X^{10} \text{ (modulo 32)}$$

Encryption

$\mathbf{m} = -1 + X^3 - X^4 - X^8 + X^9 + X^{10}$

$\mathbf{r} = -1 + X^2 + X^3 + X^4 - X^5 - X^7$

$\mathbf{e = r*h + m} = 14 + 11X + 26X^2 + 24X^3 + 14X^4 + 16X^5 + 30X^6 + 7X^7 + 25X^8 + 6X^9 + 19X^{10}$ (modulo 32)

Decryption

$\mathbf{a = f*e} = 3 - 7X - 10X^2 - 11X^3 + 10X^4 + 7X^5 + 6X^6 + 7X^7 + 5X^8 - 3X^9 - 7X^{10}$ (modulo 32)

$\mathbf{b = a} = - X - X^2 + X^3 + X^4 + X^5 + X^7 - X^8 - X^{10}$ (modulo 3)

$\mathbf{c = fp*b} = - 1 + X^3 - X^4 - X^8 + X^9 + X^{10}$ (modulo 3)