양자 내성 암호
개요

IT융합공학부 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

양자컴퓨터

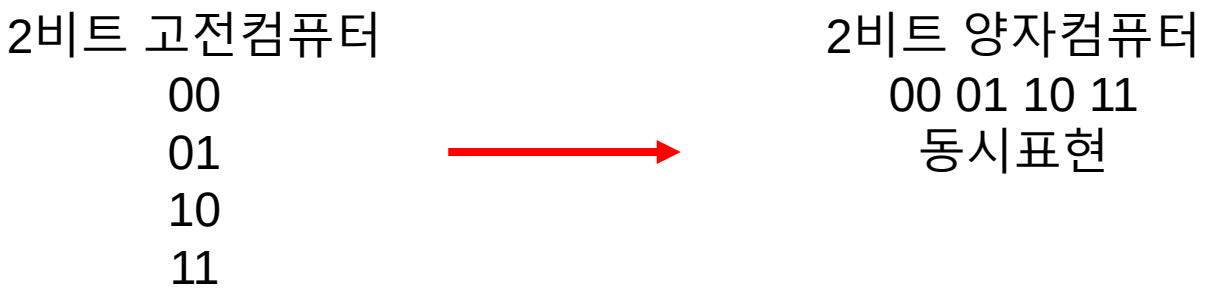
양자 내성 암호

기반 문제

CryptoCraft LAB

양자컴퓨터

- 전기신호 0, 1을 사용하는 고전컴퓨터
- 양자의 **중첩상태**를 사용하는 양자컴퓨터
  - 연산속도가 매우 빠름
  - 큐비트(qubit)



양자컴퓨터

- 현존 암호는 **수학적 난제**에 기반
- 양자컴퓨터의 성능은 난제를 깨뜨릴 수 있음
  - RSA: 소인수분해의 어려움
  - ECC: 이산대수문제의 어려움
  - 블록암호는 키 길이를 증가시키는 것으로 안전

양자 내성 암호

- Post Quantum Cryptography(PQC)
  - 후 양자 암호, 양자 내성 암호, 양자 암호
- NIST에서 양자 내성 암호 표준화를 위해 공모전 진행중
  - 21년까지 Round 3를 진행
  - 22~24년 표준화 발표

양자 내성 암호

보안 레벨	설명
1	**AES128의 보안 강도**
2	**SHA256의 충돌 내성**
3	**AES192의 보안 강도**
4	SHA384의 충돌 내성
5	AES256의 보안 강도

- 3레벨까지는 필수로 만족

양자 내성 암호

- 양자 내성 암호는 **5종류의 문제**에 기반
  - Lattice
  - Hash
  - Multivariate
  - Codes
  - Isogeny
- 각각의 방식별로 장단점 존재
  - **어느 한 방식이 일방적으로 뛰어나다고 할 수 없음**

기반 문제

Lattice (격자)

- Shortest Vector Problem(SVP), Closest Vector Problem(CVP)
  - SVP: 가장 짧은 벡터 찾기의 어려움
  - CVP: 가장 가까운 벡터 찾기의 어려움
- **연산 속도가 빠름**
- 보안레벨 만족을 위한 매개변수 설정의 어려움

기반 문제

$$\mathcal{L} = \mathcal{L}(\mathbb{B}) = \mathbb{B} \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} c_i \mathbf{b}_i : c_i \in \mathbb{Z} \right\}.$$

$\mathbb{B} = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ 는 basis of $\mathcal{L}$

- Lattice의 정의
  - n차원 공간 R에서 점이 규칙성을 지니고 격자 모양으로 배치되어 있는 것
  - 각각의 점을 **격자점(Lattice Point)**라 칭함
- 격자점은 특정 패턴을 지니고 무한히 반복
  - **패턴은 기저벡터(Basis Vector)에 의해 결정**
- Basis Vector는 무한하므로 Lattice의 형태는 매우 다양해짐

기반 문제

Hash (해시)

- 현재 사용중인 해시 기반 알고리즘
  - 해시 함수의 충돌 발생이 어렵다는 점에 기반
- **안전성 증명 가능**
- 서명 사이즈가 큼

기반 문제

Multivariate (다변수)

- 많은 변수를 사용한 다항식
  - 변수를 다항 시간 내로 찾기 어려움
- **단순함, 빠른 연산 속도**
- 키 사이즈가 큼

기반 문제

Code (부호)

- 행렬 연산을 사용
  - 의도적인 오류 주입
  - 오류를 모르면 풀기 어려운 유형의 문제
- **빠른 연산 속도**
- 키 사이즈가 큼

기반 문제

$$Hx^T = 0$$

- 이진행렬 H가 존재
  - x: linear code
  - x 존재시, H는 parity-check matrix(홀짝 검사 행렬)
- 신호 전송시 **오류가 포함**되면 **복호화가 어려움**
  - error-correcting code가 필요
- linear code 중, Goppa code가 존재
  - **기약 다항식**(irreducible polynomial) 사용
  - **다항식 정보가 있다면 효과적인 오류 정정 가능**
  - 다항식 정보가 없을 때 효과적인 오류 정정 알고리즘은 아직 없음

기반 문제

Isogeny (타원곡선)

- Supersingular elliptic curve 사용
  - 두 개의 타원 곡선의 **isogeny 관계**를 구하는 문제
- **작은 키 사이즈**
- 느린 연산 속도