격자 기반 암호 기초

임세진

https://youtu.be/Lzv3DdUx1vI

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

01. 격자 기반 암호

- 양자내성암호 (PQC : Post-Quantum Cryptography)

- 기존 암호의 비트 보안 강도를 늘리는 방법으로 양자 알고리즘을 대비 X
- 수학적 NP-Hard 난제를 기반으로 양자컴퓨터로도 해독 불가능한 보안성 획득
- 암호키 교환, 데이터 암·복호화, 무결성 인증 등 다양한 기술 제공

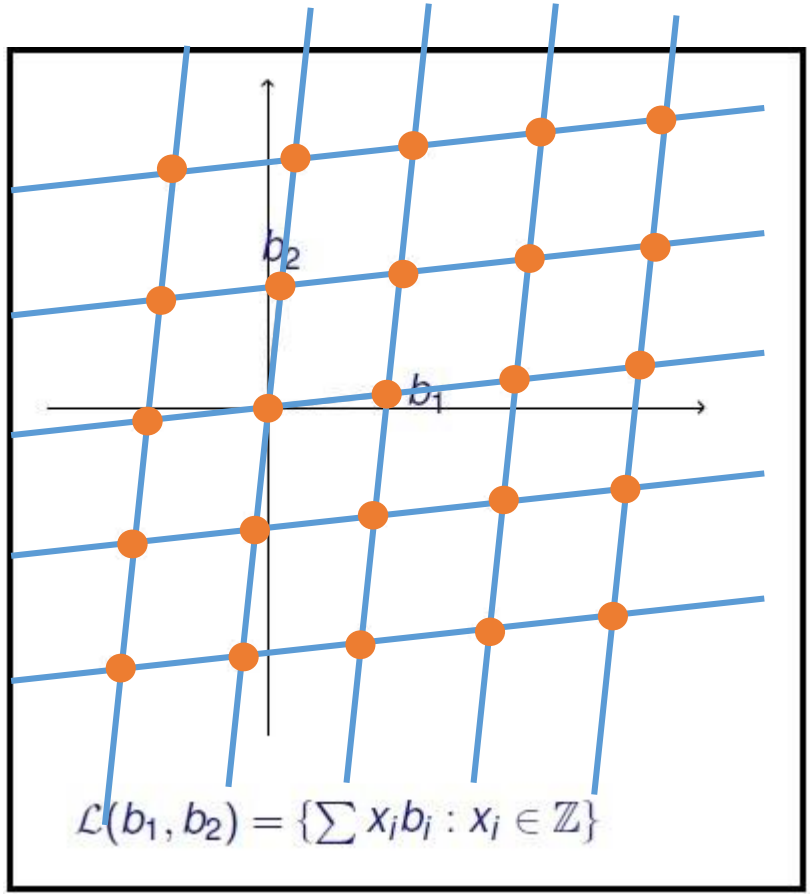
01. 격자 기반 암호

- 격자기반암호 (Lattice-based Cryptography)

- 격자 (Lattice)

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

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



n = 2 일 때

02. 격자 이론의 난제

- **고전적 격자 난제**

- SBP (Smallest basis problem) : 좋은 기저(직교에 가장 가까운 기저)를 찾는 문제. 기저는 유일하지 않음

- SVP (Shortest Vector Problem) : 격자 L이 주어졌을 때, 최소의 길이를 주는, 0이 아닌 벡터 찾기

  n(차원)이 클수록 찾기 어려움. 100차원 이하까지는 풀 수 있음.

- CVP (Closest Vector Problem) : 격자 L과 한 점이 주어졌을 때, 그 점에서 가장 가까운 격자 벡터 찾기

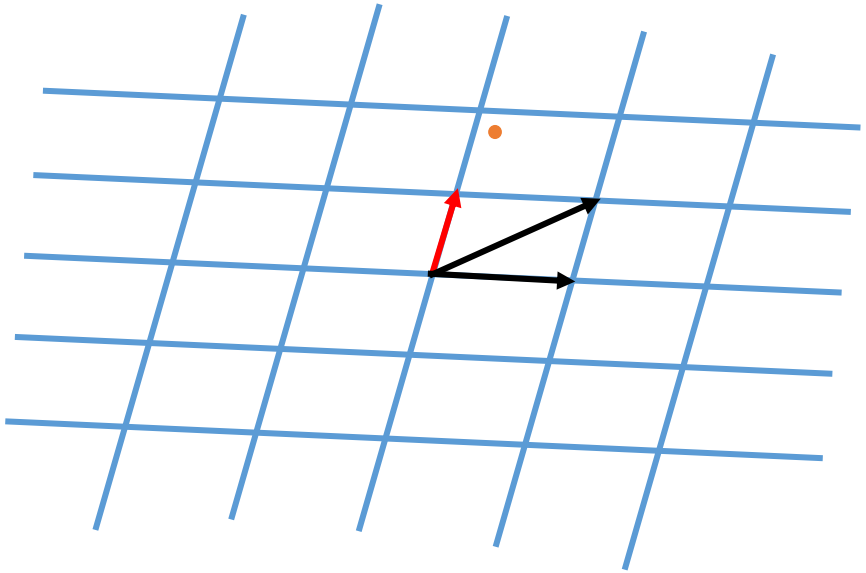
  2^n개의 후보. 차원이 커질수록 찾기 어려움

➔ 거의 직교인 기저가 있으면 이 난제들은 쉽게 풀림

✓ 격자를 주려면 기저를 줘야하는데 기저를 잘못주면 문제가 쉬워짐

✓ 어떤 경우에 문제가 쉬워지는지 정확하게 측정하기 어려움

✓ 매우 나쁜 기저를 줘도 한두번의 연산으로 쉬운 기저가 나오기도 함



02. 격자 이론의 난제

- 최근의 난제 : WC = AC equiv (Worst Case Average Case equivalent). 암호에 사용

- LWE (Learning With Errors)

  행렬을 푸는 것을 Learning이라고 함. LWE는 에러가 있는 곳에서 행렬을 푸는 것을 의미

  - 현재 가장 널리 사용되는 난제
  - 작은 에러를 포함한 연립선형방적식의 해를 구하는 문제 (에러가 없으면 쉬운 문제)
  - A와 As + e 가 주어졌을 때, s를 찾는 문제

Mod 10

0	5	2	3
1	3	6	9
3	0	8	5
4	7	9	3
1	0	6	5
4	9	2	7

X

x_1
x_2
x_3
x_4

=

6
1
0
8
2
3

➔

x_1
x_2
x_3
x_4

찾기 쉬움

Small error
(unknown)

Mod 10

0	5	2	3
1	3	6	9
3	0	8	5
4	7	9	3
1	0	6	5
4	9	2	7

X

x_1
x_2
x_3
x_4

+

0
9
1
1
0
9

=

6
1
0
8
2
3

➔

x_1
x_2
x_3
x_4

찾기 어려움

03. PQC 응용

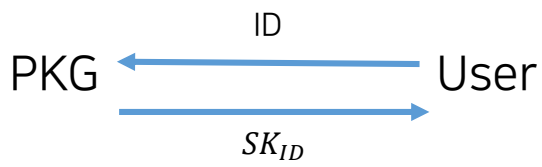
- ID 기반 암호 및 서명

해당 사용자에게만 해당하는 유일한 정보 ex) 이메일 주소, 전화번호

- ID 기반 암호 (Identity-based Encryption, IBE)
  - 사용자의 정보를 공개키로 이용하는 공개키 암호
  - 문제점 : Public Key ➔ Secret Key (누구나 생성 가능)

    기관 : MSK ➔ MPK or Public parameter

  - PKG(Private Key Generator) 필요



- ID 기반 서명 (Identity-based Signature, IBS)
  - ID 기반 암호와 같이 사용자의 정보를 공개키로 이용하는 전자서명

03. PQC 응용

- **공동인증서**
  - ✓ 서명 : RSA2048, SHA256(SHA-2) 사용
- TLS (Transport Layer Security)
  - ✓ 인터넷에서 정보를 암호화하여 송수신하는 표준 네트워크 프로토콜
  - ✓ 대칭키 암호로 데이터 암호화, 공개키 암호로 키교환 및 인증 수행
- **블록체인 – 채굴 및 Proof of Work (PoW)**
  - ✓ 거래 인증 시 전자서명 사용. 전자서명에 사용되는 알고리즘이 깨지면(SK를 알아내면) 공격자도 거래 가능
  - ✓ 크지 않은 PQC Signature 필요

➔ 양자컴퓨터 등장 시 현재 암호화 알고리즘이 깨짐 ➔ 양자 내성 암호를 적용한 방식으로 대체 요구

감사합니다