격자기반암호&코드기반암호

https://youtu.be/A7OJedPpzzs

IT융합공학부 송경주

한성대학교
HANSUNG UNIVERSITY

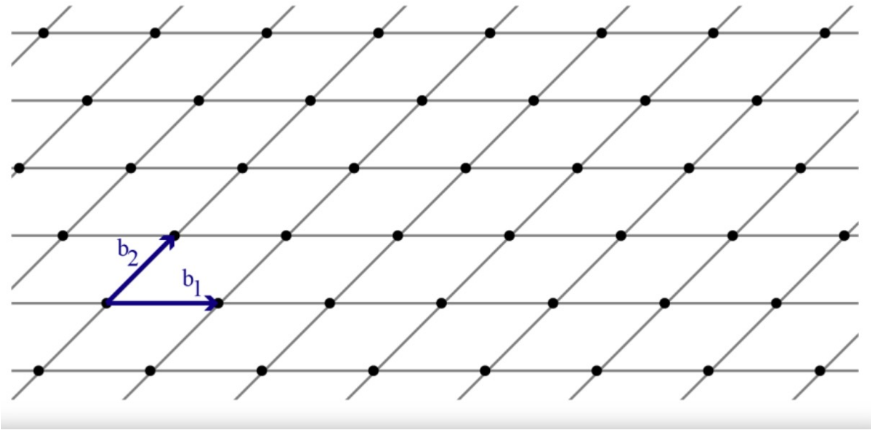
CryptoCraft LAB

격자기반암호(Lattice-based Cryptography)

- Lattice (L) 란?
  - n차원 공간인 R^n 에서 점(point)들이 규칙적인 격자무늬 배열로 배치되어 있는 상태 (i.e. norm, dimension, orthogonality, linear transformation 등과 같은 개념을 사용할 수 있음)

$$L(b_1, \dots, b_n) = \left\{ \sum_{i=0}^{n} x_i b_i | x_i \in \mathbb{Z} \right\}$$

  - 다음 식과 같이 Lattice (L)은 basis matrix (b)의 선형조합으로 이루어짐
  - Lattice(L) 의 모든 벡터가 정수 공간에 있는 경우, 정수 격자(integer lattice)라고 함



Lattice는 basis vector들의 선형결합으로 만들 수 있는 점들로 이루어짐
(그러므로 lattice 모양은 basis vector들로 결정)

*basis vector : n차원 공간인 R^n 내의 임의의 원소들을 표현하기 위한 최소한의 벡터(기본 벡터)

격자기반암호(Lattice-based Cryptography)

- Lattice-based Cryptography ?

: Lattice 상의 수학적 난제인 Hard Lattice Problem을 암호 기법에 적용시킨 것!

- 1996년, Ajtai는 Lattice Problem의 NP-hardness를 증명하였음

(Lattice에서 vector을 다항 시간 내에 찾는 알고리즘이 없음)

- 1997년, Ajtai-Dwork은 최초로 worst case assumption(최악의 시나리오)를 기반으로 한 최초의 암호를 구현을 함

(worst case assumption을 기반으로 한 최초의 구현이었기 때문에 암호화에서 특별한 역할이 됨)

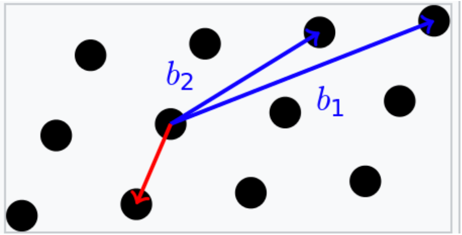
- 2005년, Oded Regev가 제안한 Learning with Errors(LWE)을 기반으로 한 공개키 암호가 처음으로 안전성이 검증되었음.

격자기반암호(Lattice-based Cryptography)

- Lattice-based Cryptography

: 수백 차원 lattice 상에서 임의의 위치(공개 키와 연관)와 가장 가까운 점(개인 키와 연관)을 찾는 어려움을 기반으로 함

→ Lattice 상의 수학적 난제가 암호 security의 기반이 된다!



최단거리 벡터 문제 : 기저벡터 b_1, b_2 에서 최단 거리 (빨간색) 벡터를 찾기 어려움

$$Classic\ 격자\ 난제 \begin{cases} \text{Shortest Vector Problem (SVP)} \\ \text{Closest Vector Problem (CVP)} \\ \vdots \end{cases}$$

* SVP : Lattice L이 주어지면 원점과 가장 가까운 0이 아닌 벡터 벡터 v를 찾음 : $||v-t|| \leq \gamma\lambda_n(L)$
* CVP : Lattice L과 target point t 가 주어지면 t 에서 가장 가까운 벡터 v를 찾음 : $||v-t|| \leq \gamma\ dist(t, L)$

$$Cryptography\ 격자\ 난제 \begin{cases} \text{Learning With Errors (LWE)} \\ \text{Small Integer Solution(SIS)} \end{cases}$$ → 가장 많이 사용

- LWE 및 SIS은 SVP로 축약(reduction) 가능 : LWE, SIS 문제를 해결할 경우 SVP 문제 해결 가능

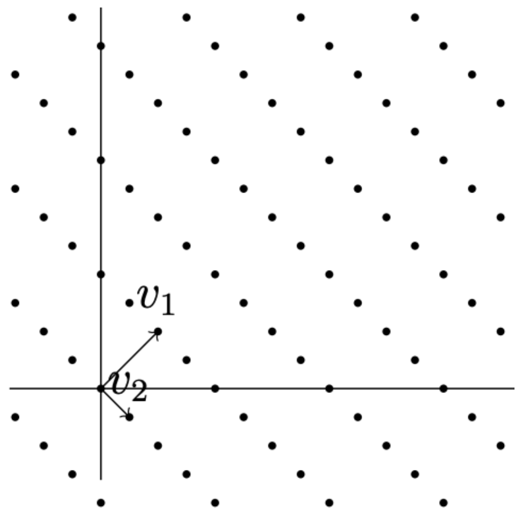
격자기반암호(Lattice-based Cryptography)

- Lattice-based Cryptography

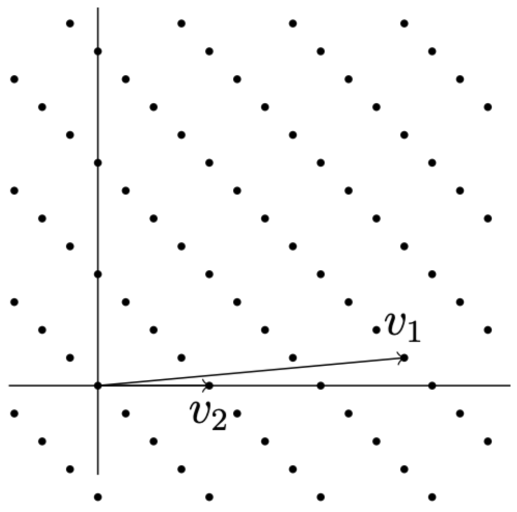
[GGH/HNF public key cryptosystem] - closest vector problem (CVP)

→암호 시스템의 설계 핵심 : basis의 직교성(orthonormality)

- 개인키 : Hadamard 비율 1에 가까운(거의 직교하는) 벡터로 구성된 basis 벡터 B_{priv} (good orthonormality)
- 공개키 : Hadamard 비율 0에 가까운(직교하지 않는) 벡터로 구성된 B_{priv} (bad orthonormality)



두 basis vector v_1, v_2 가 거의 orthonormal
(Good basis)



두 basis vector v_1, v_2 가 거의 orthonormal 하지 않음
(bad basis)

격자기반암호(Lattice-based Cryptography)

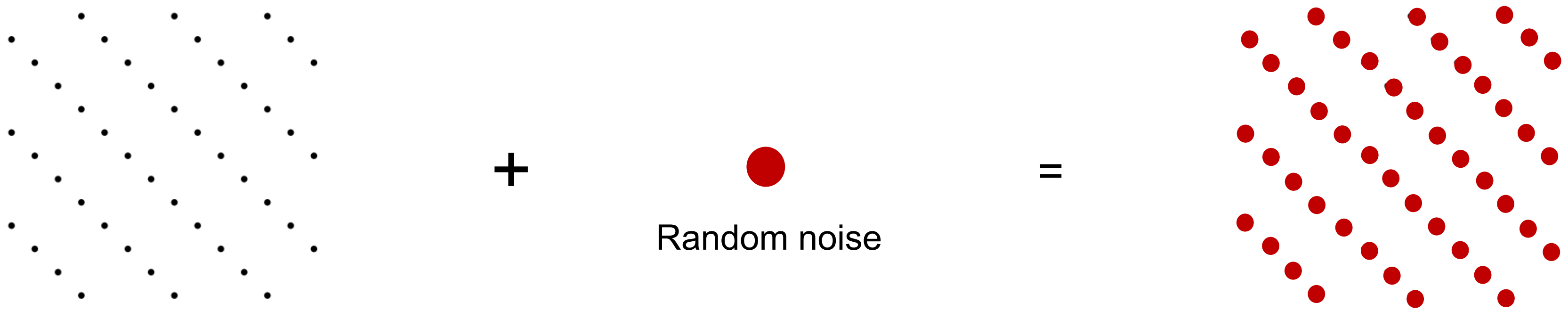
- Lattice-based Cryptography

[GGH/HNF public key cryptosystem] - closest vector problem (가장 가까운 벡터를 찾는데 어려움을 기반)

Encryption : Lattice point v에 random noise을 추가 하여 암호화

message $m = m_1, \ldots, m_n$, error e, public key $B' = b_0, \ldots, b_n$ 가 주어지면, 다음과 같이 암호화 진행

$$v = \sum m_i b'_i \,, \qquad c = v + e = m \cdot B' + e$$



Decryption : 대상 암호 c = (r mod H) = v + r 에서 가장 가까운 lattice point v 와 error vector r = c - v를 찾아 복호화

$$c \cdot B^{-1} = (m \cdot B' + e)B^{-1} = m \cdot U \cdot B \cdot B^{-1} + e \cdot B^{-1} = m \cdot U + e \cdot B^{-1}, m = m \cdot U \cdot U^{-1}$$

→ 이 방식은 1999년 Nguyen이 모든 암호문이 평문에 대한 정보를 드러내며 복호화 문제는 일반 CVP보다 쉽게 해결할 수 있어 암호화 체계에 결함이 있음을 보였음

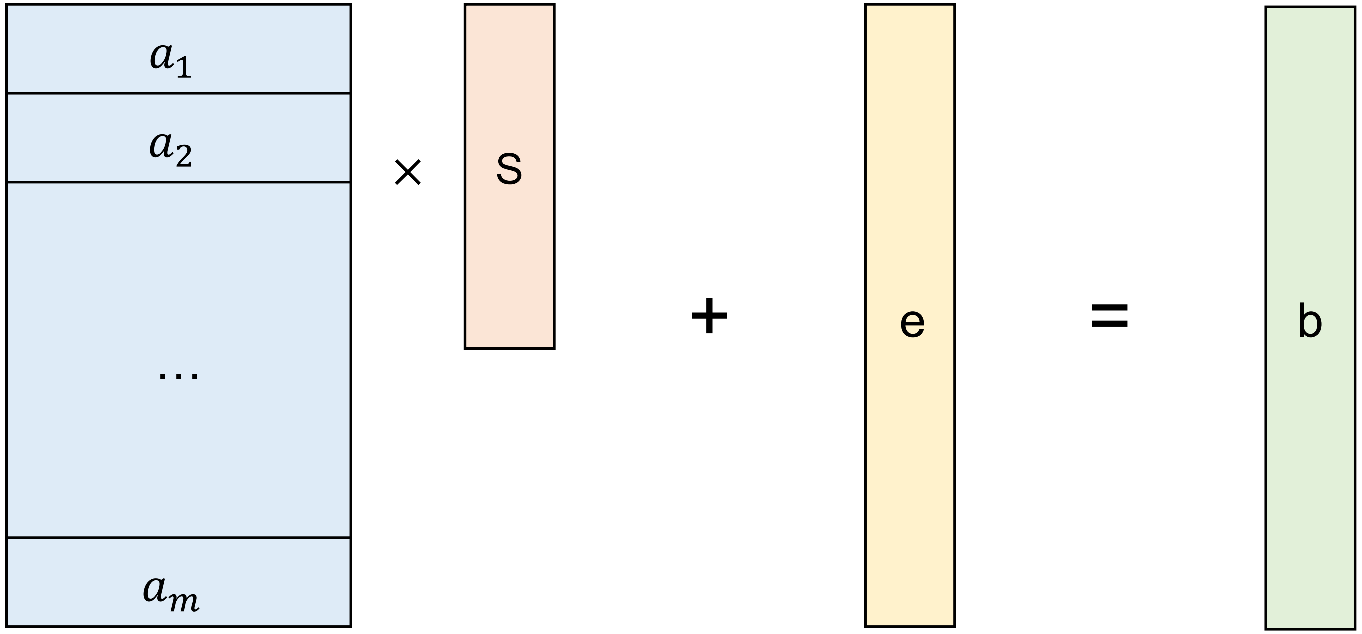
격자기반암호(Lattice-based Cryptography)

- Lattice-based Cryptography

[LWE(Learning With Errors)]

LWE problem : 랜덤한 integer matrix $A = (a_1, \ldots, a_m),\ A \in Z_q[n \times m]$, Secret key $s \in Z_q[m \times 1]$, 작은 임의의 랜덤 error $e \in Z_q[n \times 1]$ 라고 가정,

→ $A = (a_1, \ldots, a_m)$와 e가 주어졌을때, A에 secret key(=vector)를 곱한 후 e를 더하면 행렬 A를 알고 있더라도 결과 벡터 b에서 s를 복구하는 것의 어려움을 기반으로 함



코드기반암호(code-based cryptography)

- Code-based cryptography?

: NP-hard로 간주되는 알려지지 않은 오류 수정 코드를 디코딩하는 문제를 기반으로 함

$$C_0 = H\boxed{e^T}$$

- 암호문, 공개키, Hamming weight는 알려진 정보 : $C_0, H, wt(e)$
- 특정 Hamming weight가 주어졌을 때, 이를 만족하는 벡터 e 를 찾아내는 문제

H(공개키) 생성에 대한 정보(개인키)를 가지고 있으면 암호문 C_0으로 부터 원본 벡터 e 복구 가능

코드기반암호(code-based cryptography)

- Code-based cryptography

가장 잘 알려진 Code-based cryptography로는 두가지가 있음

1. 1978년 Robert McEliece 가 제안한 McEliece cryptosystem
2. 1986년 Harald Niederreiter 가 제안한 Niederreiter cryptosystem

F_2: The filed with two elements
C : a binary code of length n and dimension k
G : $k \times n$ generating matrix
H : $(n-k) \times n$ parity check matrix, $GH^T = 0$
$s = Hc^T$: syndrome

- McEliece : 평문 x에 공개키 G를 곱한것에 Hamming weight $w_H(e) = t$ 를 가지는 에러 e를 더함 : $y = xG + e$.

→암호문 y, 공개키 G, Hamming weight $w_H(e) = t$ 가 주어졌어도 에러 e를 찾는 것은 매우 어려운 문제

- Niedderreiter : 주어진 평문의 Hamming weight가 $w_H(x) = t$를 만족하도록 조절하여 공개키 H와 곱함: $y = Hx^T$

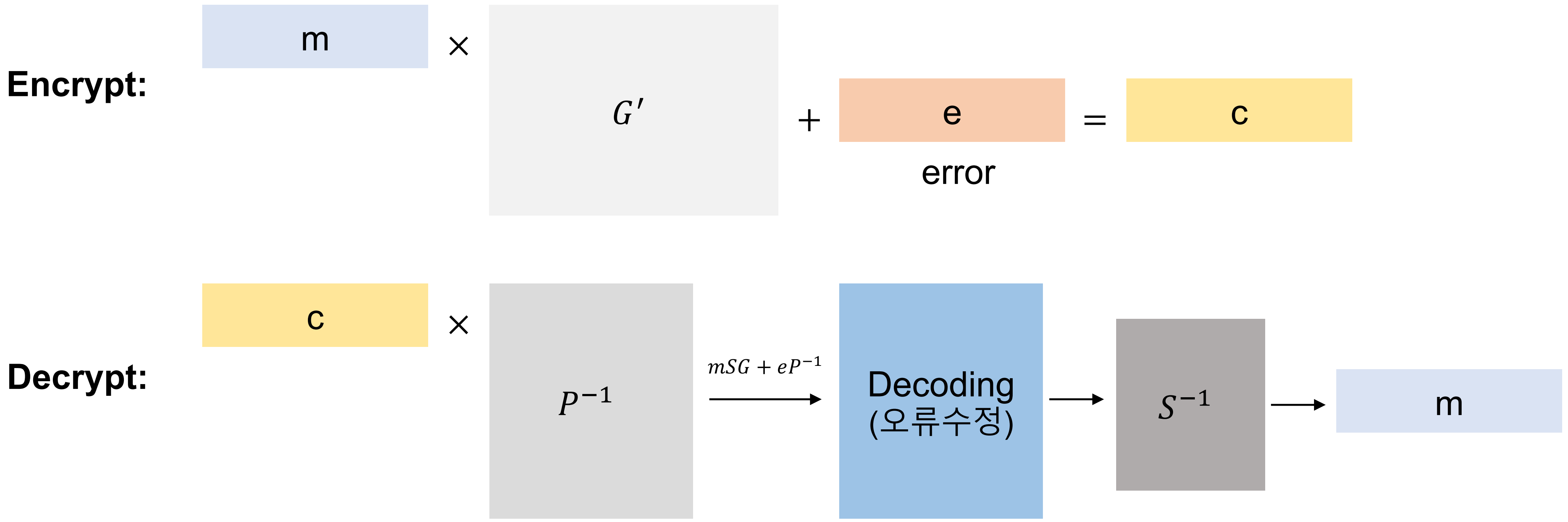
→ 암호문 y, 공개키 H, Hamming weight $w_H(x) = t$ 가 주어졌어도 평문 x를 찾는 것은 매우 어려운 문제

	McEliece	Niederreiter
Public Key	G	H
Plaintext	$x \in F_2^k$	$x \in F_2^n, \quad w_H(x) = t$
Ciphertext	$y = xG + e, \quad w_H(e) = t$	$y = Hx^T$
Ciphertext space	F_2^n	F_2^{n-k}

코드기반암호(code-based cryptography)

- McEliece cryptosystem
  - $G' = SGP$ (공개키) , $G: generator\ matrix$
  - Encryption : Generator matrix $G' = SGP$, $c = mG' + e$
  - Decryption : $cP^{-1} = mSG + eP^{-1}$, mS is obtained by decoding, $mSS^{-1} = m$

S : random $(k \times k)$ nonsingular binary matrix
G : $(k \times n)$ generator matrix of a t-error-correcting binary linear code
P: random $(\mathrm{n} \times n)$ permutation matrix
Private key : S, G, P
Public key : $G' = SGP$



코드기반암호(code-based cryptography)

- 코드기반 암호에 대한 대표적 공격법

1. ISD(information set decoding) : 코드기반 암호에 대해 가장 효율적인 공격법

$$C_0 = He^T$$

- 공개키 H와 암호문 C_0 만으로 원본 메시지를 복구 → 메시지 자체를 복구하는 공격, 개인키를 찾지 않음

2. Structure attack
   - 공개키 H로 부터 구조적 결함을 찾아 개인키 자체를 복구하는 공격
   - ISD 보다 성능이 좋지 않아 잘 연구되지는 않음

Q & A