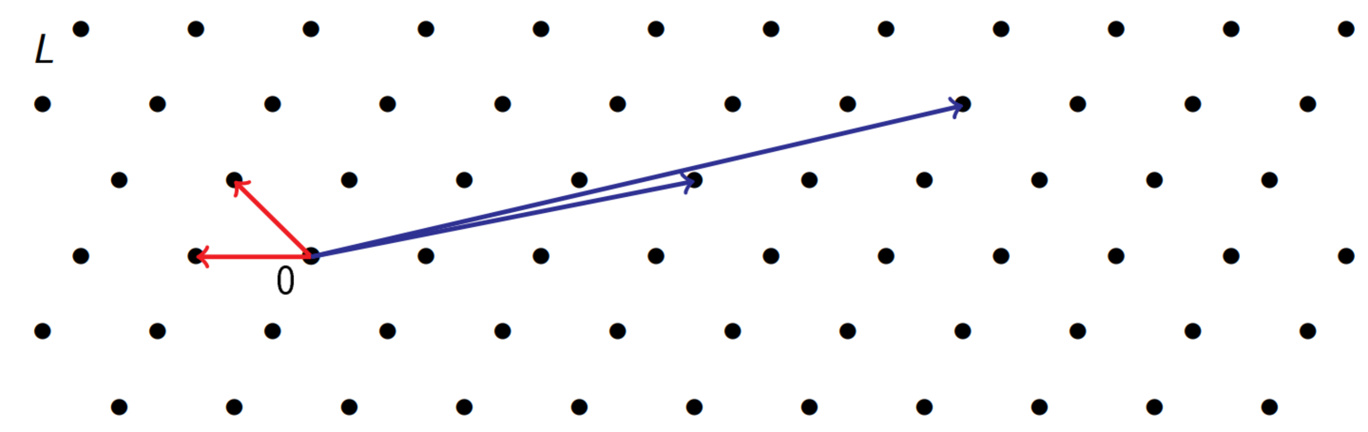
격자기반 암호

목차

1

격자란 무엇인가?

격자(lattices)



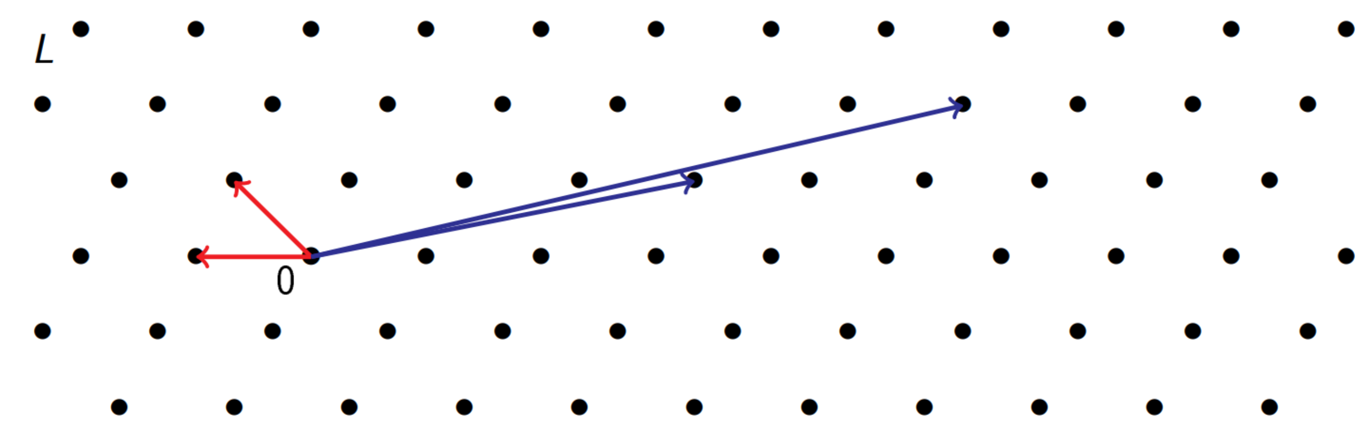
$$L = \mathcal{L}(B) = \langle B \rangle = \{Bx \mid x \in \mathbb{Z}^n\}, B \in \mathbb{Z}^{m\times n}$$

B : Basis matrix of rank n

n : rank m: dimension

$n = m$: Full rank lattice

격자(lattices)

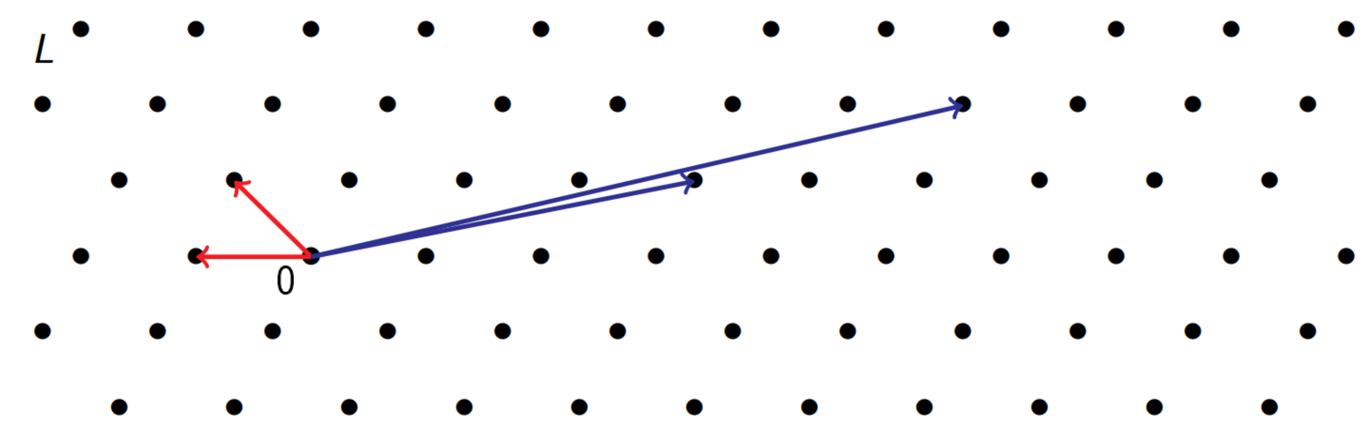


$\lambda_1(L)$: Shortest length of $x \in L$

$\mathrm{Vol(L)} = \det(B)$

$\lambda_1(L) \approx \mathrm{Vol}(L)^{1/n}$

격자(lattices)

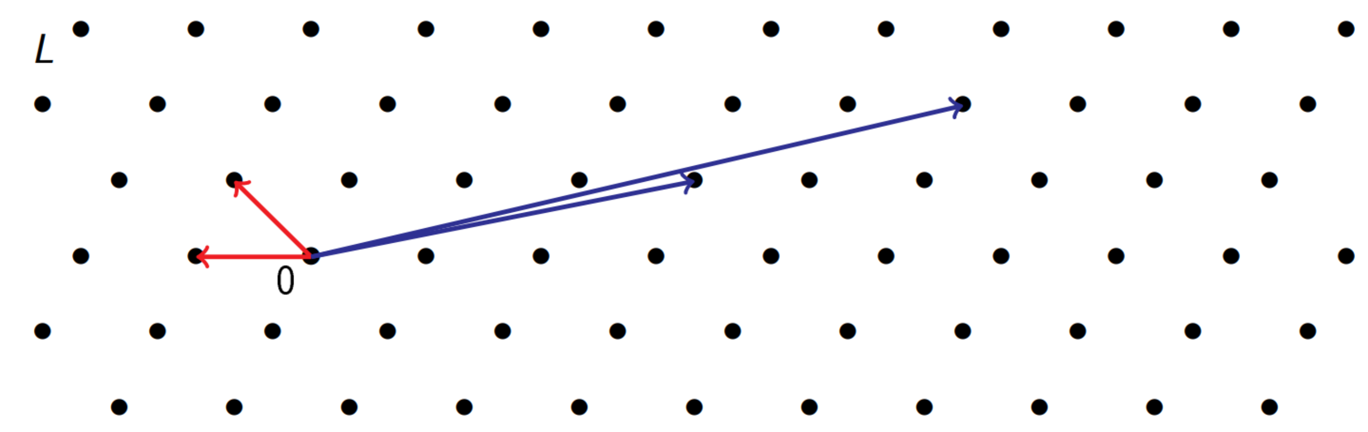


예제:

$$\left\langle \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix} 8 & 9 \\ 12 & 2 \\ 1 & 0 \end{pmatrix} \right\rangle$$

$$\left\langle \begin{pmatrix} 3 & 5 & 8 \\ 1 & 2 & 3 \end{pmatrix} \right\rangle \text{ :Generating set}$$

격자(lattices)



-격자의 베이시스는 유일할까?

-두 격자가 같은지 여부는 어떻게 체크할 수 있을까?

격자의 베이시스

$$\left\langle \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix} \right\rangle$$

$$\begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -4 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -7 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -4 & -7 \\ 1 & 2 \end{pmatrix}$$

격자의 베이시스

일반적으로

$$\langle B_0 \rangle = \langle B_1 \rangle \Leftrightarrow B_0 = B_1 U, \quad B_1 = B_0 V \Rightarrow B_0 = B_0 U V$$

$$I = UV \Rightarrow det(U) * det(V) = 1 \Rightarrow det(U) = \pm 1$$

결론적으로

$$L = \mathcal{L}(B) = \mathcal{L}(B \cdot U); U \in Z^{n \times n}, det(U) = \pm 1$$

격자는 굉장히 많은 베이시스를 갖는다.

-Basis 는 어떻게 표현할까?
-좋은 Basis matrix는 무엇일까?

격자의 베이시스 표현법

Hermite normal form : 삼각행렬의 표현법

$$\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$$

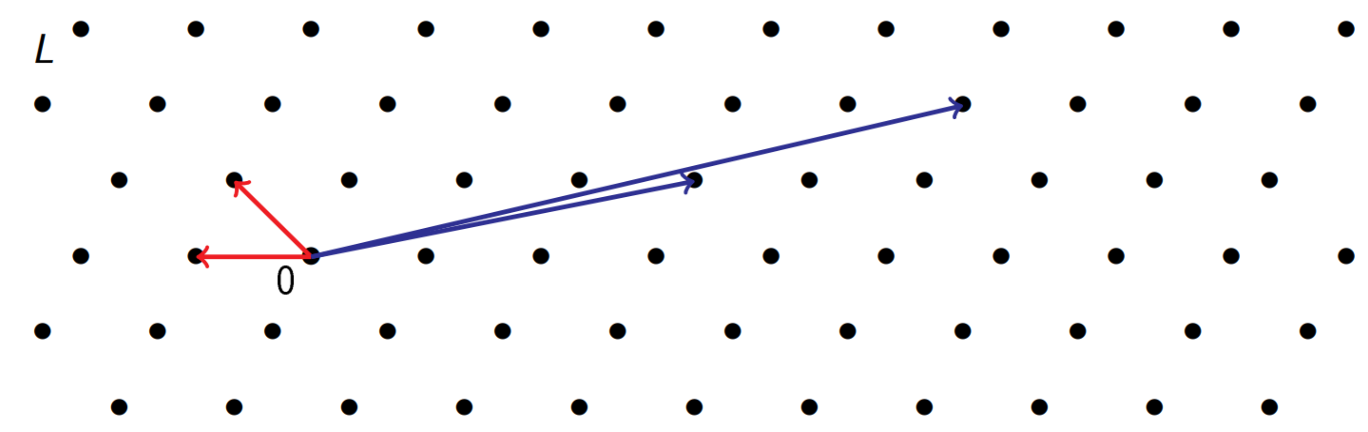
QR decomposed form : Gram-Schmidt 좌표에서 삼각화 표현법

$$\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} \frac{3}{\sqrt{10}} & -\frac{1}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} & \frac{3}{\sqrt{10}} \end{pmatrix} \cdot \begin{pmatrix} \sqrt{10} & \frac{17}{\sqrt{10}} \\ 0 & \frac{1}{\sqrt{10}} \end{pmatrix}$$

HKZ reduced form : 크기가 작은 벡터들로 이루어진 표현법

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Good basis v.s. Bad basis

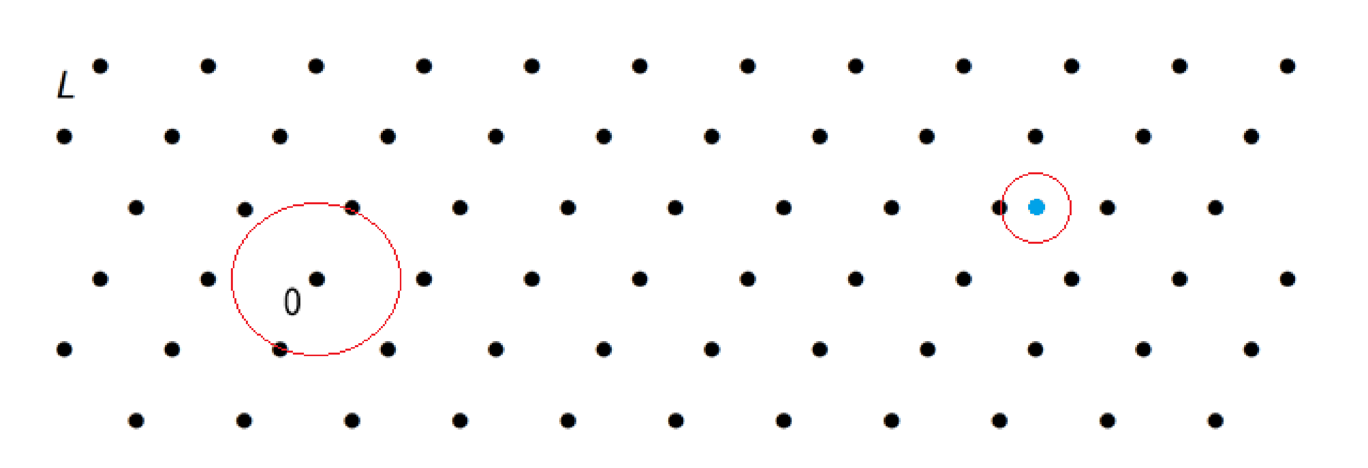


Good basis: 짧은 벡터들로 이루어진 베이시스
Bad basis: 긴 벡터들로 이루어진 베이시스

Good basis $\Rightarrow$ Bad basis : easy

Good basis $\Leftarrow$ Bad basis : hard

격자의 짧은 벡터, 가까운 벡터



SVP: Shortest vector problem

Input: 베이시스 메트릭스

Output: 가장 짧은 길이의 벡터

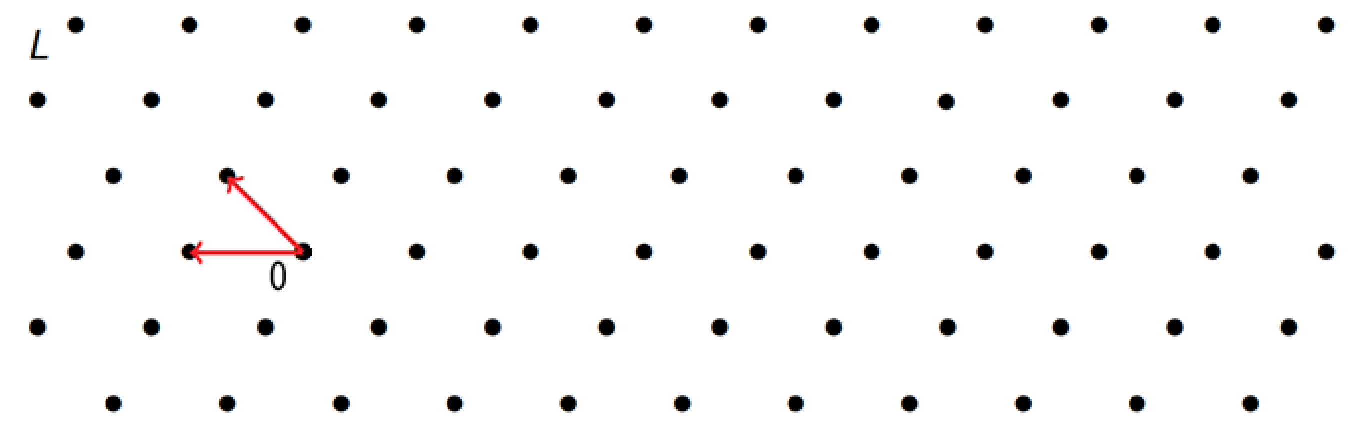
특이점: 해가 유일하지 않음

CVP: Closest vector problem

Input: 베이시스 메트릭스+ vector t

Output: t에 가장 가까운 벡터

격자의 다양한 문제들 (1)

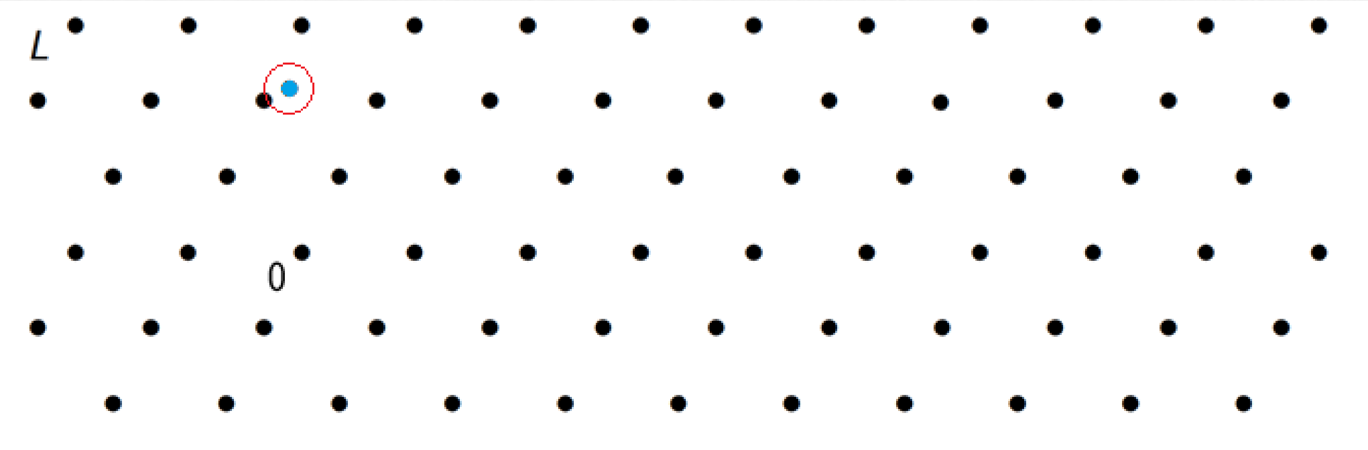


SIVP: Shortest independent vector problem

Input: 베이시스 메트릭스

Output: 가장 짧은 길이의 벡터들

격자의 다양한 문제들 (2)



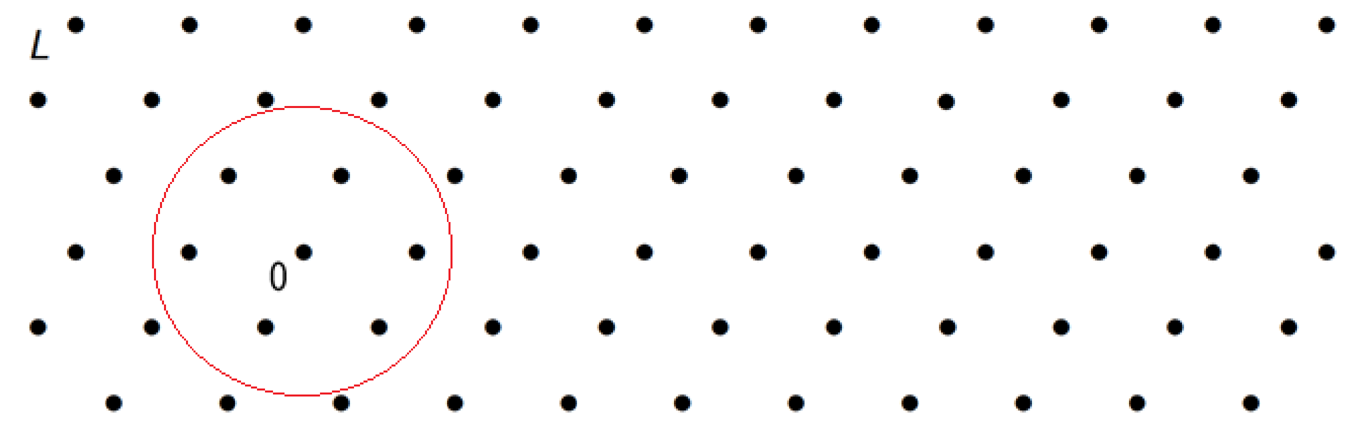
BDD: Bounded distance decoding

Input: 베이시스 메트릭스 + vector t s.t $\mathrm{dist}(\mathrm{L},\mathrm{t}) < \mathrm{d}$

Output: t에 가장 가까운 벡터

특이점: 해가 유일

격자의 다양한 문제들 (3)

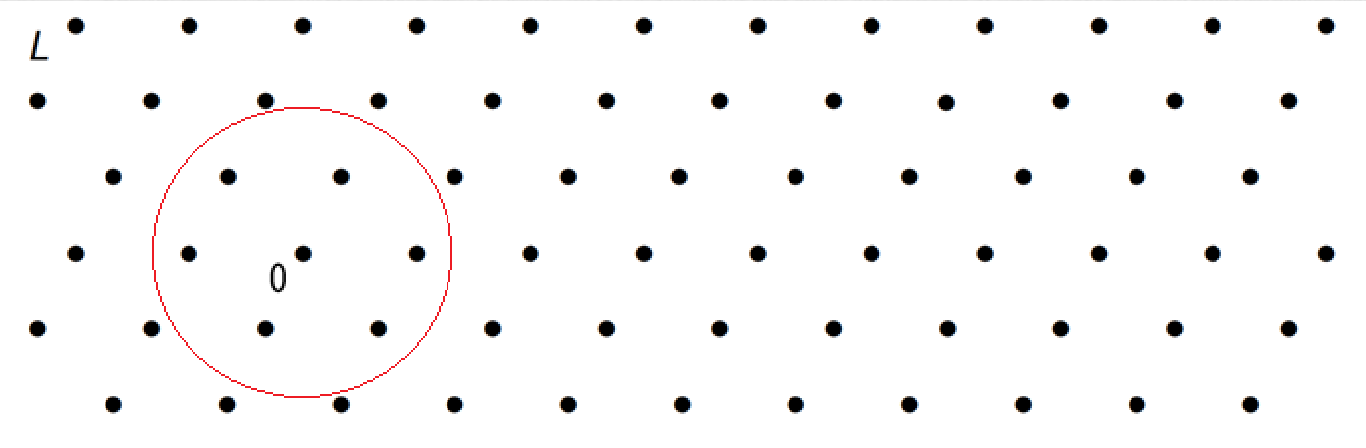


γ-SVP: γ-approximate shortest vector problem

Input: 베이시스 메트릭스

Output: γ 길이 이하의 벡터

격자의 다양한 문제들 (4)

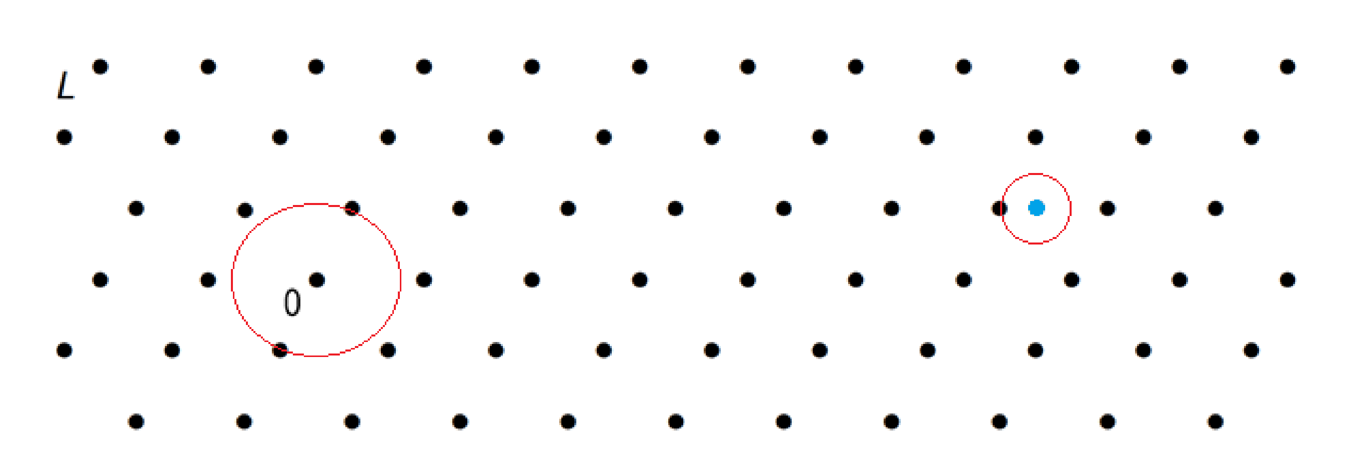


γ-Gap SVP: γ-gap shortest vector problem

Input: 베이시스 메트릭스

Output: $\begin{cases} 0 \text{ if } \lambda_1(L) < \det(B)^{1/n} \\ 1 \text{ if } \lambda_1(L) > \gamma \det(B)^{1/n} \end{cases}$

격자의 짧은 벡터, 가까운 벡터



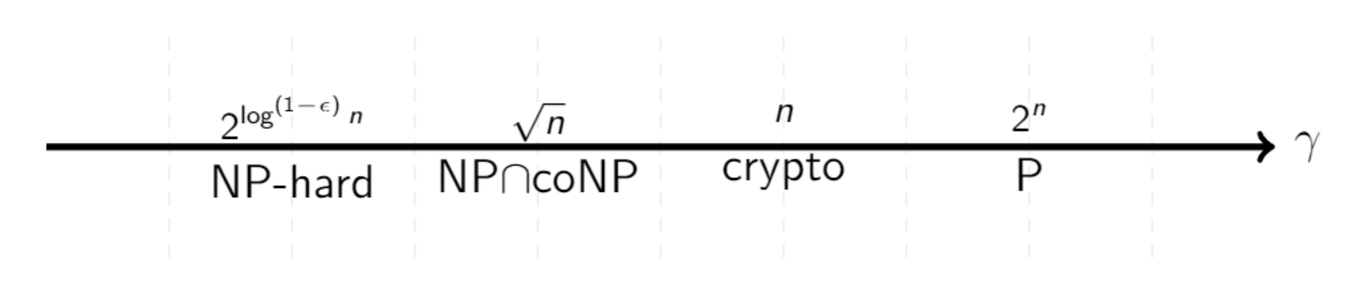
SVP: Shortest vector problem   CVP: Closest vector problem

If… a bad basis of L 가 인풋인 경우

랭크가 커질 수록 문제가 어려워짐. (NP hard)

- 현재 퀀텀 컴퓨터를 이용해도 어려움

격자의 근사 짧은 벡터 (Gap SVP)

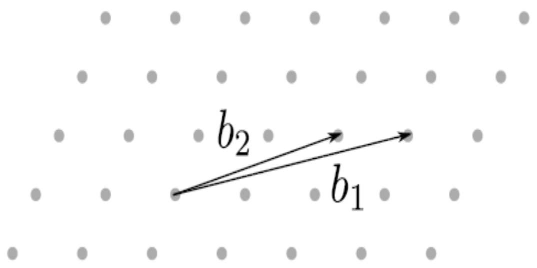


γ 가 커질수록 문제는 쉬워짐

γ 의 크기가 랭크에 대해서 지수함수인 경우 쉬움

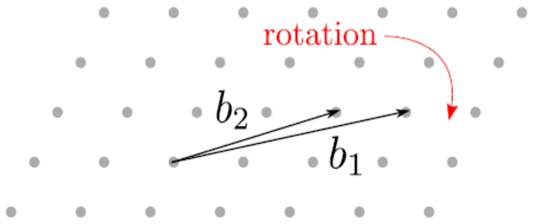
γ 현재 암호스킴을 깨려면 랭크에 관한 다항함수인 경우를 분석

격자의 짧은 벡터; 예제



$$M = \begin{pmatrix} 10 & 7 \\ 2 & 2 \end{pmatrix}$$

격자의 짧은 벡터; 예제

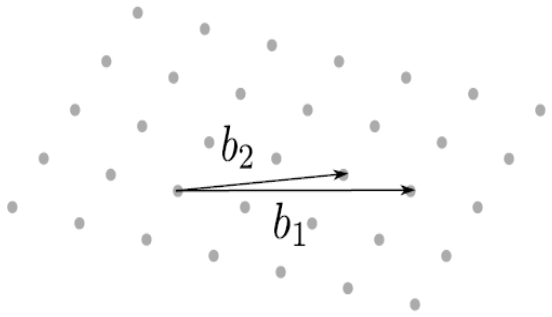


rotation

$$M = \begin{pmatrix} 10 & 7 \\ 2 & 2 \end{pmatrix}$$

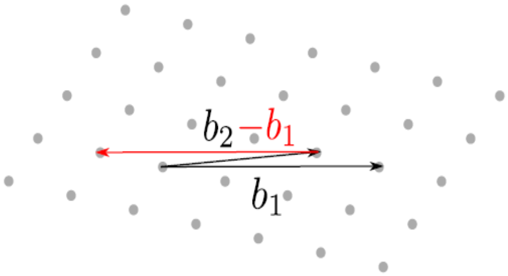
Basis change

격자의 짧은 벡터; 예제



$$M = \begin{pmatrix} 10.2 & 7.3 \\ 0 & 0.6 \end{pmatrix}$$

격자의 짧은 벡터; 예제

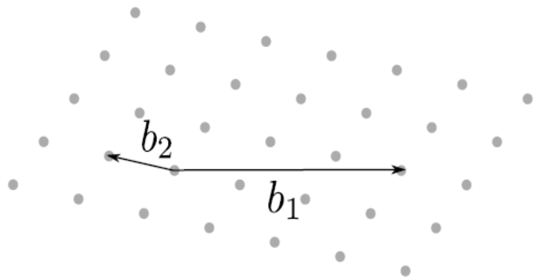


reduce b_2 with b_1

$$M = \begin{pmatrix} 10.2 & 7.3 \\ 0 & 0.6 \end{pmatrix}$$

"Euclidean division" (over $\mathbb{R}$) of 7.3 by 10.2

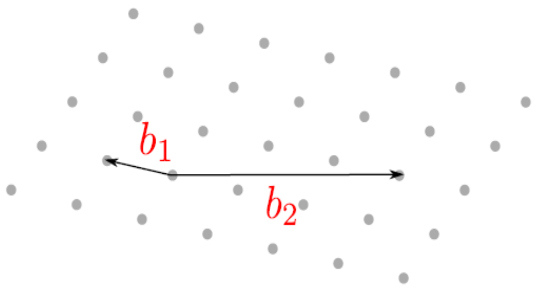
격자의 짧은 벡터; 예제



check $\|b_2\| < \|b_1\|$

$$M = \begin{pmatrix} 10.2 & -2.9 \\ 0 & 0.6 \end{pmatrix}$$

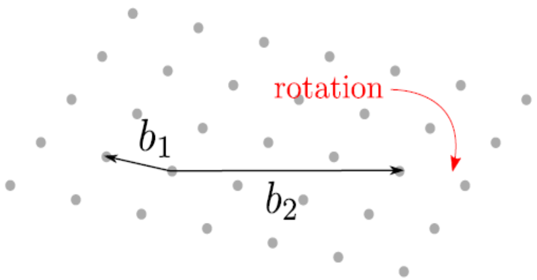
격자의 짧은 벡터; 예제



swap

$$M = \begin{pmatrix} -2.9 & 10.2 \\ 0.6 & 0 \end{pmatrix}$$

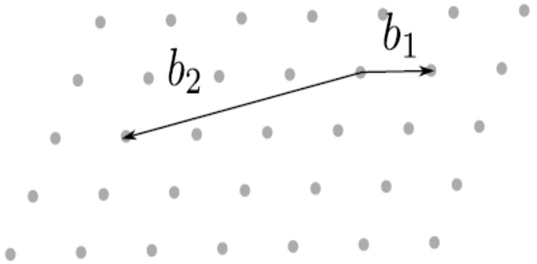
격자의 짧은 벡터; 예제



rotation

$$M = \begin{pmatrix} -2.9 & 10.2 \\ 0.6 & 0 \end{pmatrix}$$

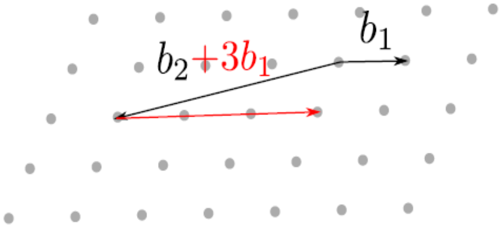
격자의 짧은 벡터; 예제



rotation

$$M = \begin{pmatrix} 3 & -10 \\ 0 & -2 \end{pmatrix}$$

격자의 짧은 벡터; 예제

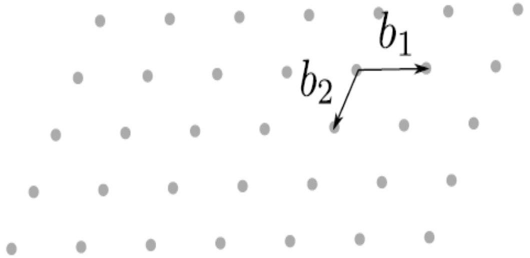


$$M = \begin{pmatrix} 3 & -10 \\ 0 & -2 \end{pmatrix}$$

reduce b_2 with b_1

"Euclidean division" (over $\mathbb{R}$) of -10 by 3

격자의 짧은 벡터; 예제



$$M = \begin{pmatrix} 3 & -1 \\ 0 & -2 \end{pmatrix}$$

If $n \geq 3$??

SVP in practice

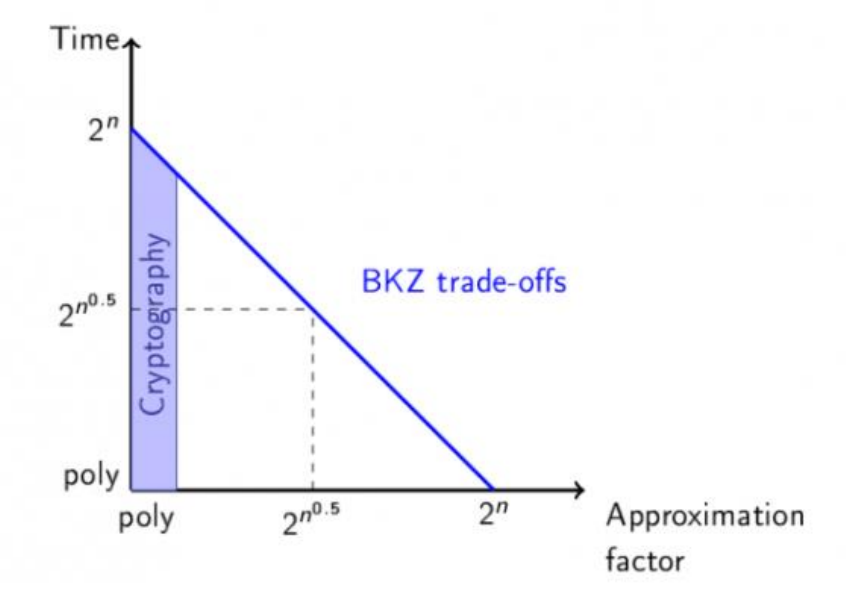
현재 SVP는 얼마나 풀 수 있을까?

$n=2$	Easy!!
$n \le 80$	A few minutes on a personal laptop
$n \le 170$	A few days on a big computer
$n \ge 500$	Cryptography

SVP Challenge: https://www.latticechallenge.org/svp-challenge/

SVP in practice

현재 SVP는 얼마나 풀 수 있을까?



https://www.esat.kuleuven.be/cosic/blog/lattice-reduction/

SVP(CVP)의 한계

- SVP (CVP)는 worst case 에 대해서 어렵다 .

  모든 레티스 베이시스에 대해서 효율적으로 SVP를
  푸는 알고리즘은 없음

  일부 레티스 베이시스에서는 문제가 쉬울 수 있음
  (ex: Good basis 가 주어진 경우)

  암호에서는 average case 에 대해서 어려운 문제가 필요함

2

격자 기반 문제

Strategy for Encryption

Goal of encryption :
-Ideally, only authorized parties can decipher a ciphertext back to plaintext and access original information

-Encryption scheme aims to prevent ciphertexts from leaking any information

How?

-One-wayness

- Pseudo-randomness

SIS (short integer solution) 문제

$$q, n, m \in \mathbb{Z},\ \mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$$

$$A \leftarrow Uniform(\mathbb{Z}_q^{m \times n})$$

find $x \in \{-1, 0, 1\}^m \setminus \{\vec{0}\}$ $\quad xA = 0$

SIS (short integer solution) 문제

One-wayness of SIS

It is hard to recover x from $\boxed{A}$

근의 존재성? $\begin{bmatrix} A \\ b \end{bmatrix} \Rightarrow \begin{bmatrix} x & -1 \end{bmatrix} \begin{bmatrix} A \\ b \end{bmatrix} = 0$

$$\boxed{b} = \boxed{x}\,\boxed{A} \approx_{\text{Leftover hash lemma}} \mathbb{Z}^n$$

LWE (Learning with errors) 문제

$q, n, m \in \mathbb{Z}$, $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$

Given A and $b = A s \mod q$

Recover s

$A \leftarrow Uniform(\mathbb{Z}_q^{m \times n})$ $\quad s \leftarrow N(0, \sigma)^n$

Easy!!

LWE (Learning with errors) 문제

$q, n, m \in \mathbb{Z},\ \mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$

Given A and $b = A\,s + e \mod q$

Recover s and e

$A \leftarrow Uniform(\mathbb{Z}_q^{m\times n})$ $\quad s\ e \leftarrow N(0,\sigma)^n$

Easy??

LWE (Learning with errors) 문제

$q, n, m \in \mathbb{Z},\ \mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$

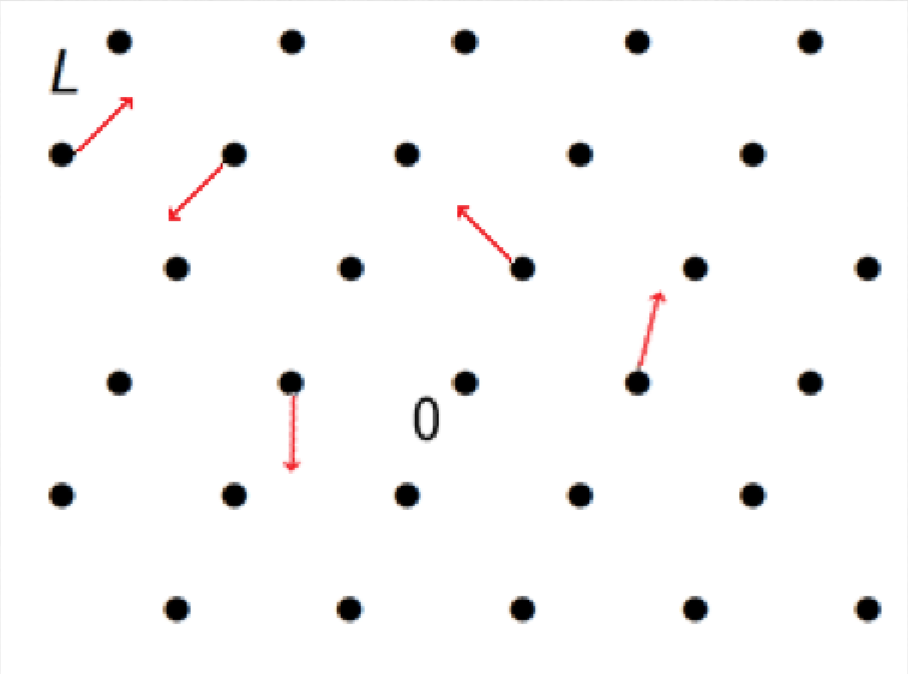
Given A and $b = A\,s + e \mod q$

Recover s and e

$A \leftarrow Uniform(\mathbb{Z}_q^{m \times n})$ $\quad s,\ e \leftarrow N(0, \sigma)^*$

Still hard

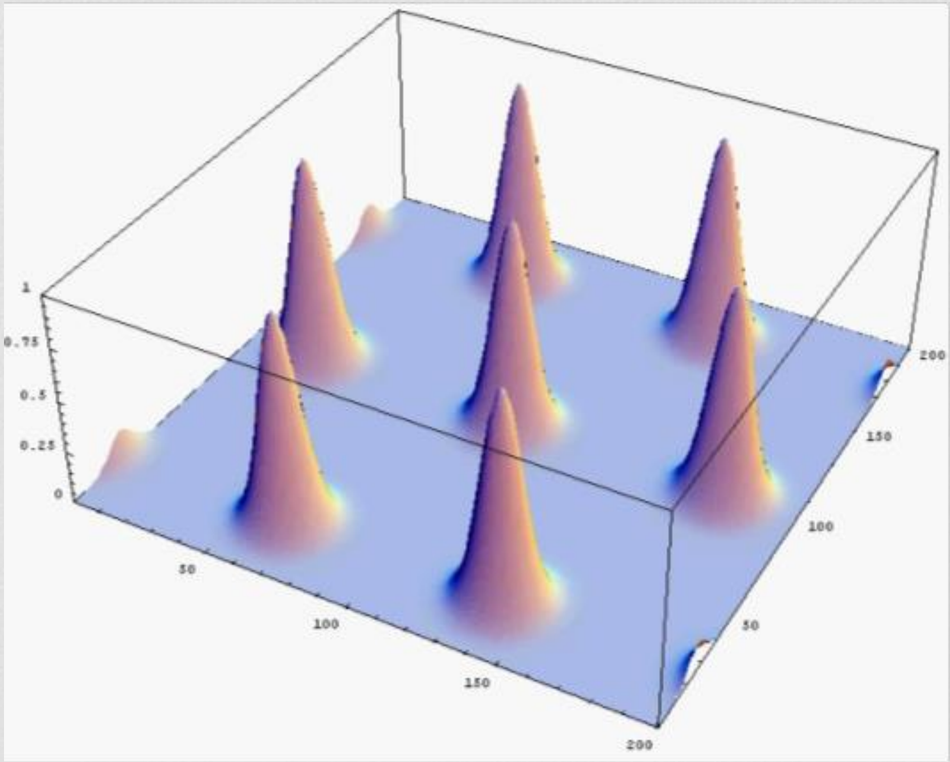
LWE (Learning with errors) 문제



$$e \leftarrow N(0, \sigma)^m$$

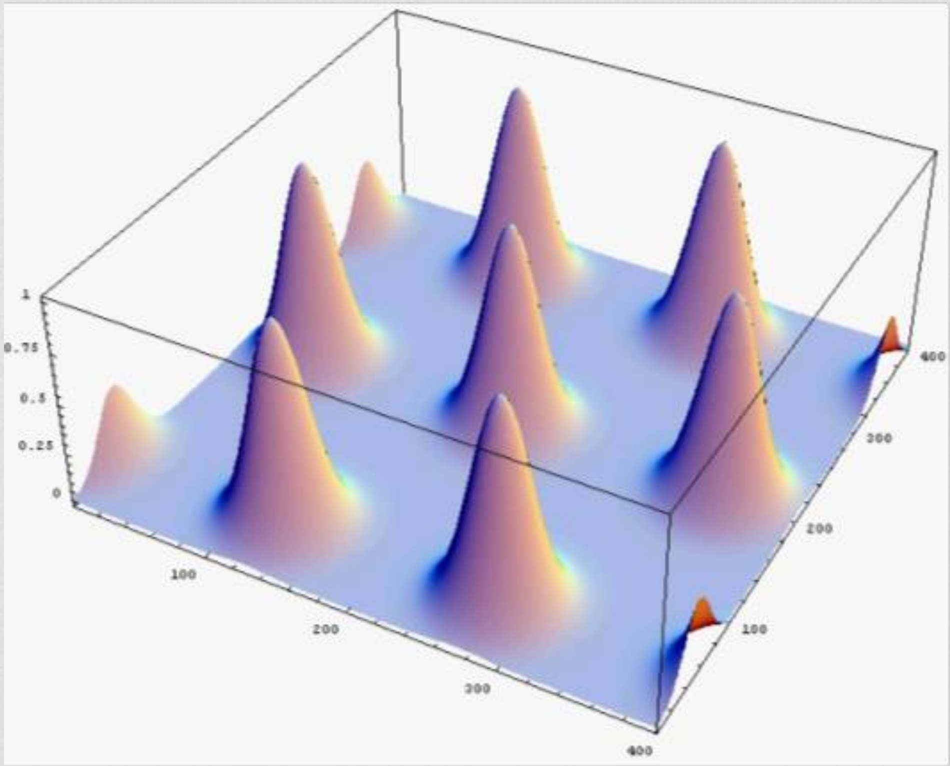
LWE (Learning with errors) 문제

Pseudo-randomness of LWE



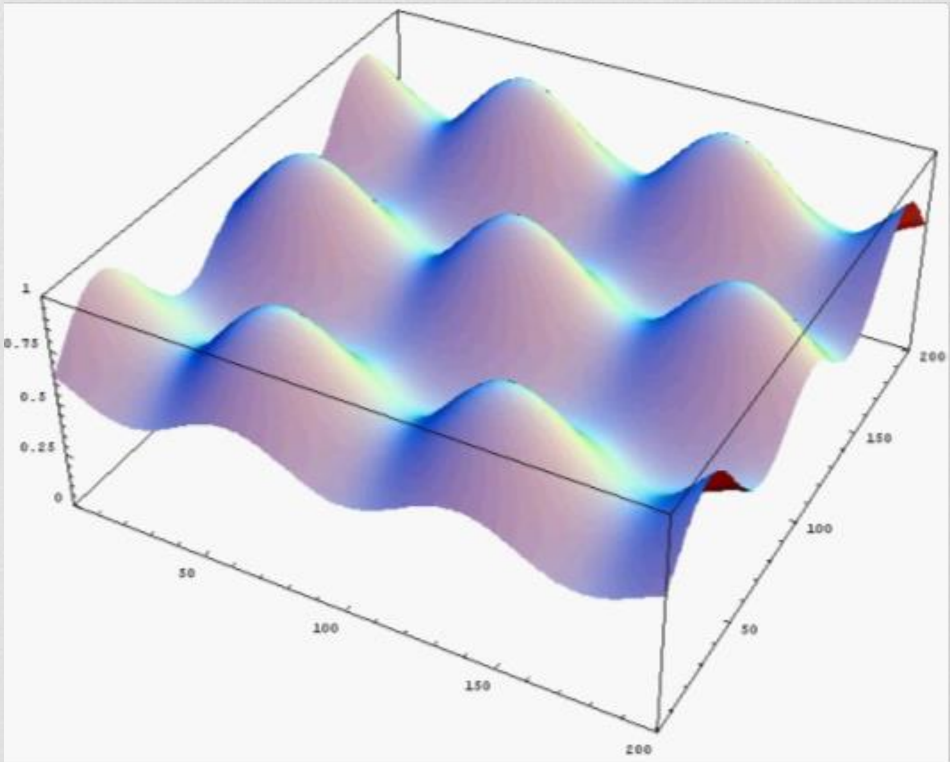
LWE (Learning with errors) 문제

Pseudo-randomness of LWE



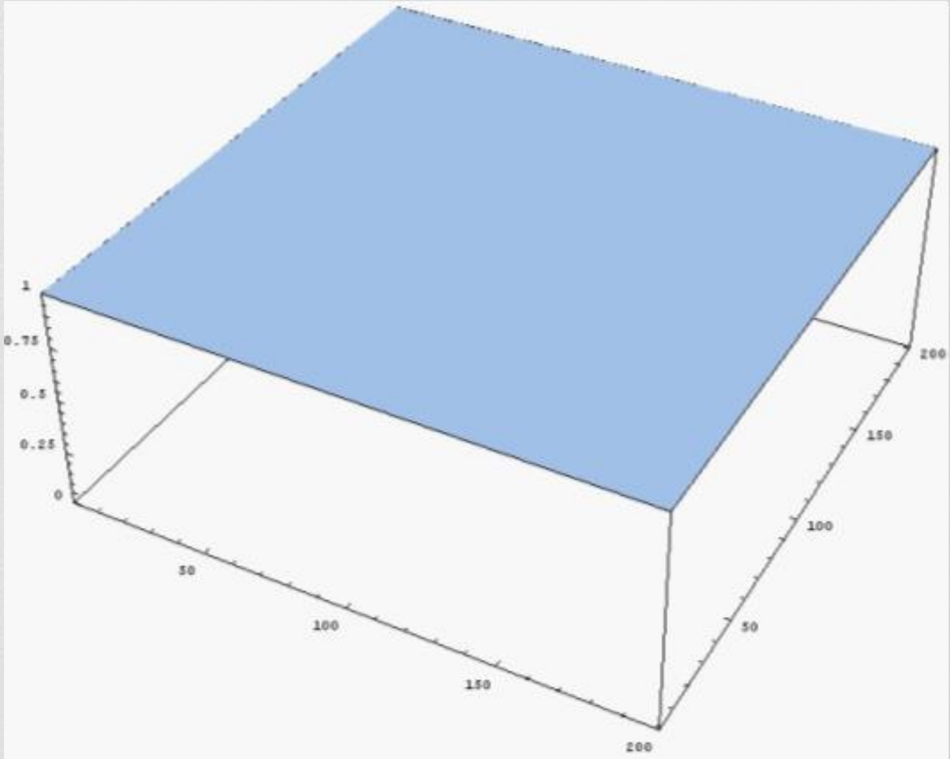
LWE (Learning with errors) 문제

Pseudo-randomness of LWE



LWE (Learning with errors) 문제

Pseudo-randomness of LWE



dLWE (decisional Learning with errors) 문제

$q, n, m \in \mathbb{Z},\ \mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$

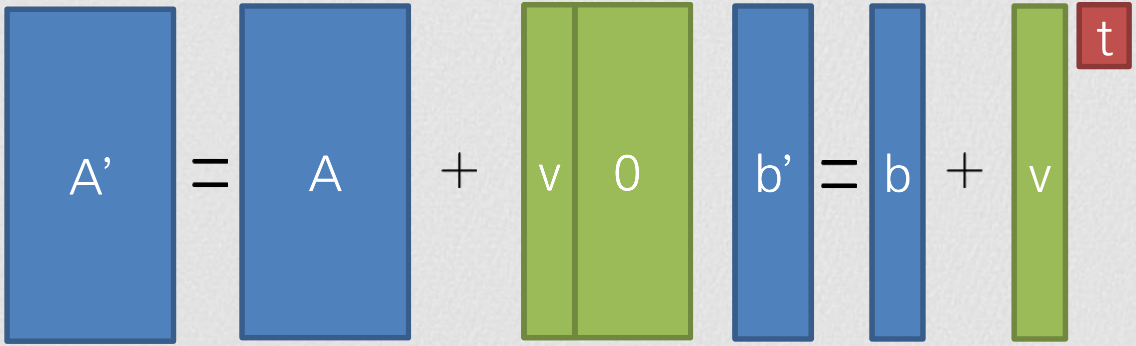
Given A and $b = A\,s + e \mod q$

or

Given A and $b \leftarrow Uniform(\mathbb{Z}_q^m)$

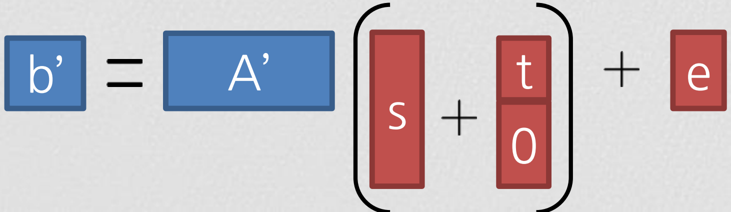
LWE와 dLWE의 관계

$\mathrm{LWE} \leq \mathrm{dLWE}$



If $t = s1$

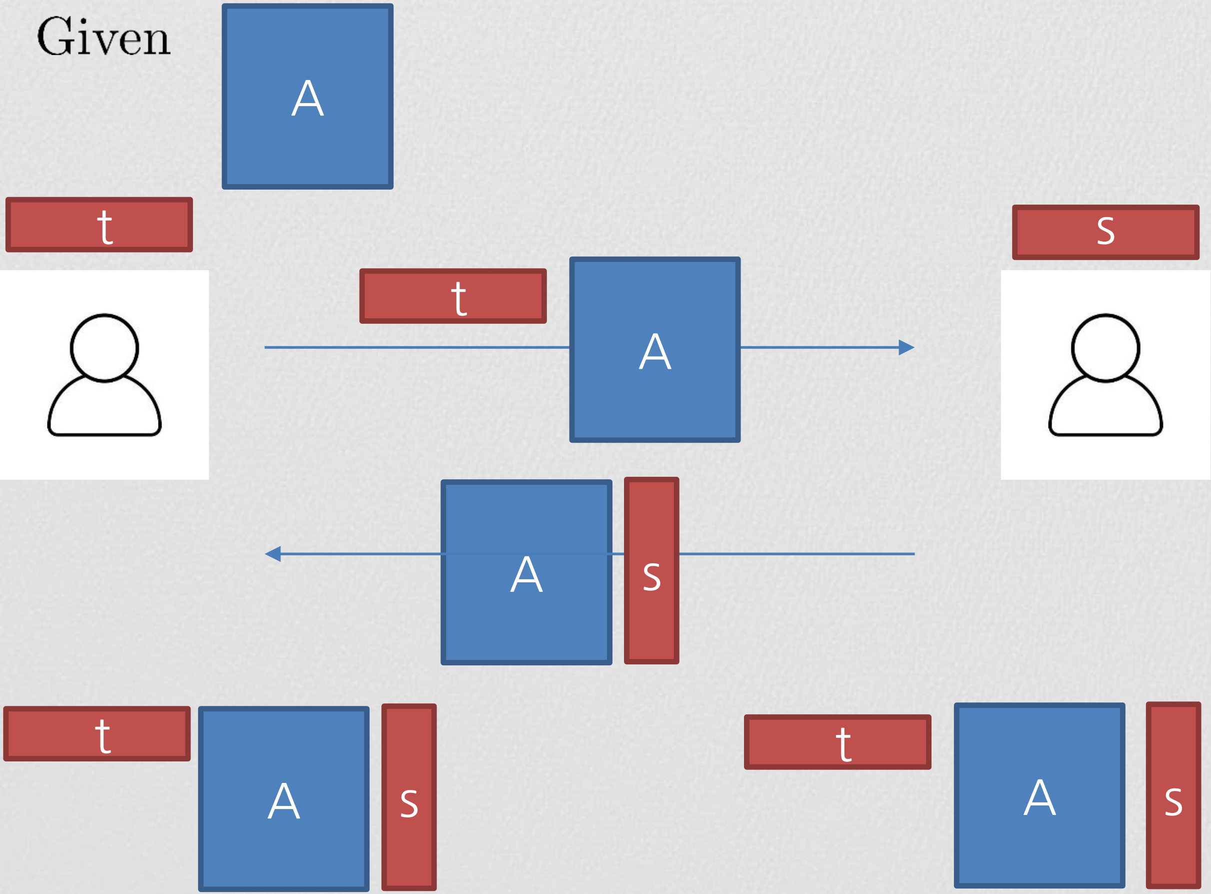
A’, b’: LWE instance



LWE 의 application

- Key exchange
- Public key Encryption
- Oblivious Transfer
- PRF
- Identity based Encryption
- ID-Based Encryption
- Homomorphic Encryption
- Attribute-Based Encryption

Warm up: LWE 기반 Key exchange



LWE

유일한 해를 가짐

알려진 공격들

- Dual attack [Alb17]
- Primal attack [AGVW17]
- BKW algorithm [KF15]
- AG algorithm [AG11]

$\mathrm{GapSVP} \leq \mathrm{LWE}$ [Reg05]

LWE (SIS) 와 SVP 의 관계

Solving SIS $\Leftrightarrow$ Solving SVP in any lattice

$L = \{x \in \mathbb{Z}^m | xA = 0 \bmod q\}$: 격자

SIS solution x: 격자 L의 가장 짧은 벡터

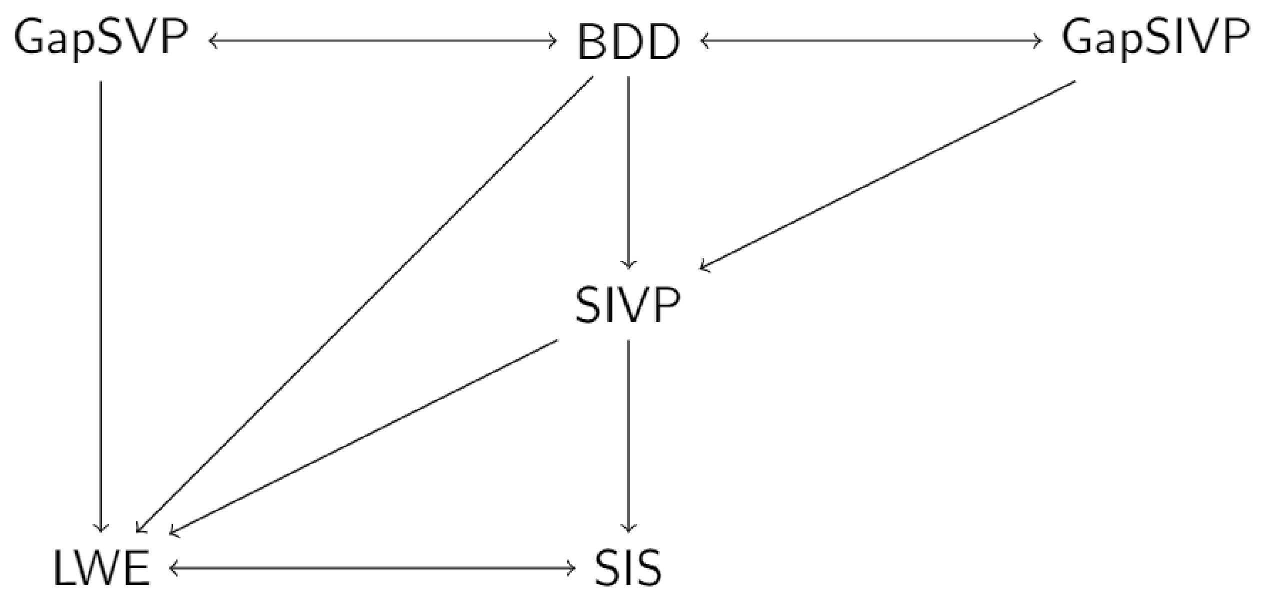
Solving LWE $\Leftrightarrow$ Solving SVP in any lattice

$L' = \{(x, y, z) \in \mathbb{Z}^{m+n+1} | bz - Ax = y \bmod q\}$

LWE solution (s, e): 격자 L'의 가장 짧은 벡터

SIS and LWE: average case problems $\Rightarrow$ Good for crypto

LWE (SIS) 와 SVP 의 관계



LWE (SIS) 는 만능?

	격자	Wish
Storage	$\tilde{O}(n^2)$	$\tilde{O}(n)$
Computing Time	$\tilde{O}(n^2)$	$\tilde{O}(n)$
Break Known attack time	$2^{\Omega(n)}$	$2^{\Omega(n)}$

It is inefficient