격자기반 암호

목차

3

격자 기반 암호

격자기반 암호란

1) 격자를 이용하여 암호를 설계하거나,
2) 격자 이론을 이용한 안전성 증명을 가능한 암호

격자기반암호	표준암호
▪ 증명 가능 안전성	▪ 안전성 증명 불가능
▪ Worst case 문제에 기반	▪ Average case 문제에 기반
▪ 양자컴퓨터에 내성	▪ 양자컴퓨터에 취약
▪ 구현의 용이함	▪ 구현이 복잡함
▪ 다양한 기능성	

증명 가능 안전성?

- 격자 기반 암호를 해독 $\Rightarrow$ SIS,LWE 문제를 해결
- SIS, LWE 문제를 해결 $\Rightarrow$ SVP, CVP (NP-hard)
- 증명 가능 안전성은 암호가 안전할거라는 강력한 증거를 제시
- 예제: One-wayness of modular squaring

$$N = pq, \quad p, q: \text{ two large primes}$$

$$f(x) = x^2 \bmod N$$

If $f^{-1}(x) = x^{1/2} \bmod N$ is computable
N can be factorable

Average case 어려움의 취약성

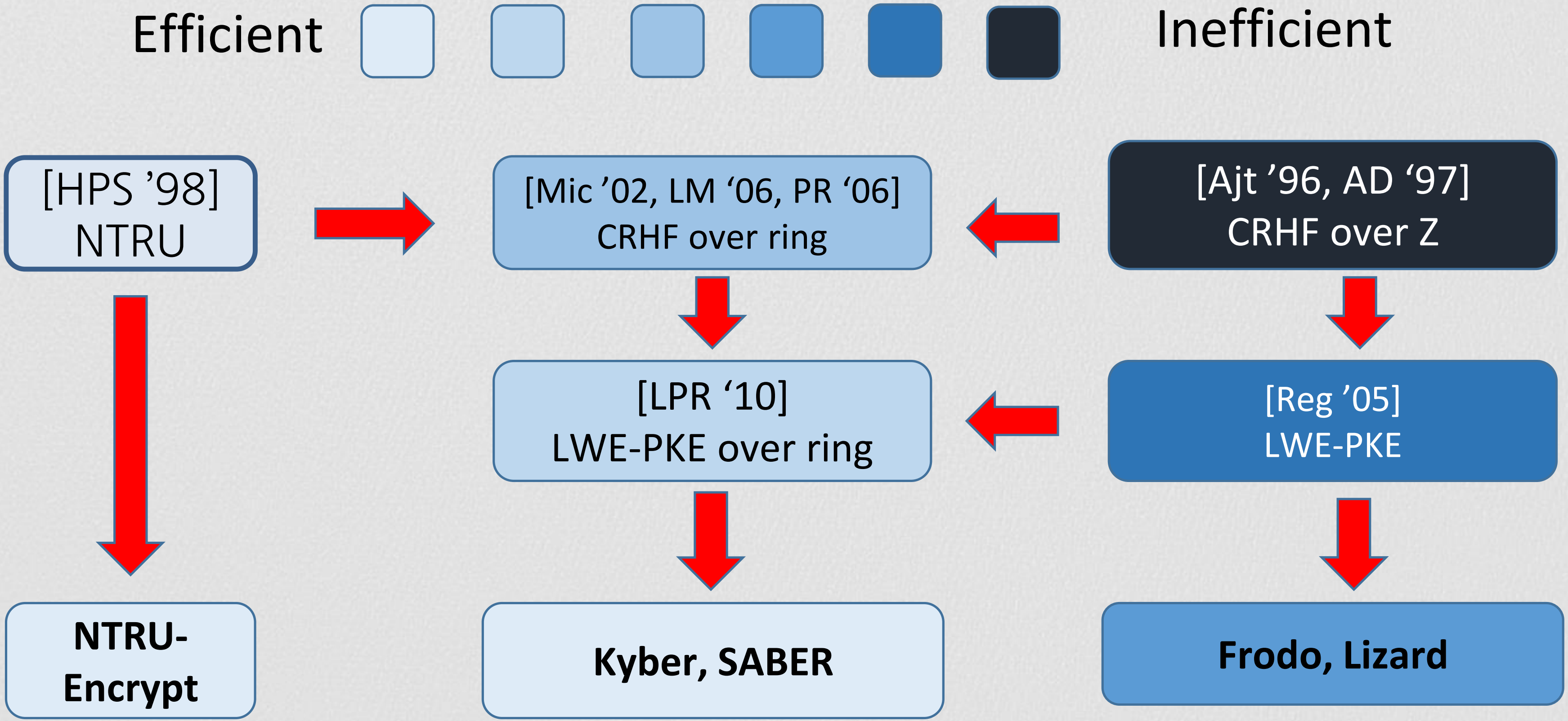
- Average case 어려움: ex) RSA; 소인수분해
- 소인수분해를 어렵게 하기 위해서 $N = pq$ 을 어떻게 설정?
- p, q 를 랜덤하게 선택하면 충분?

  $(1978)\ p-1\ \ q-1$ 이 작은 소인수로만 이루어진 경우

  $(1981)\ p+1\ \ q+1$ 이 작은 소인수로만 이루어진 경우

- 암호가 안전한지 어떻게 확인?

Encryption scheme overview



Cited from ‘Lattice Cryptography in the NIST Standardization Process’, Vadim Lyubashevsky

격자기반 암호 CRHF

- Collision - Resistant Hash Functions (CRHF)

  Input: $\{0,1\}^m$

  Output: $\mathbb{Z}_q^n$

  Hard to find collisions; $x \neq y,\ f(x) = f(y)$

- 격자 기반 CRHF

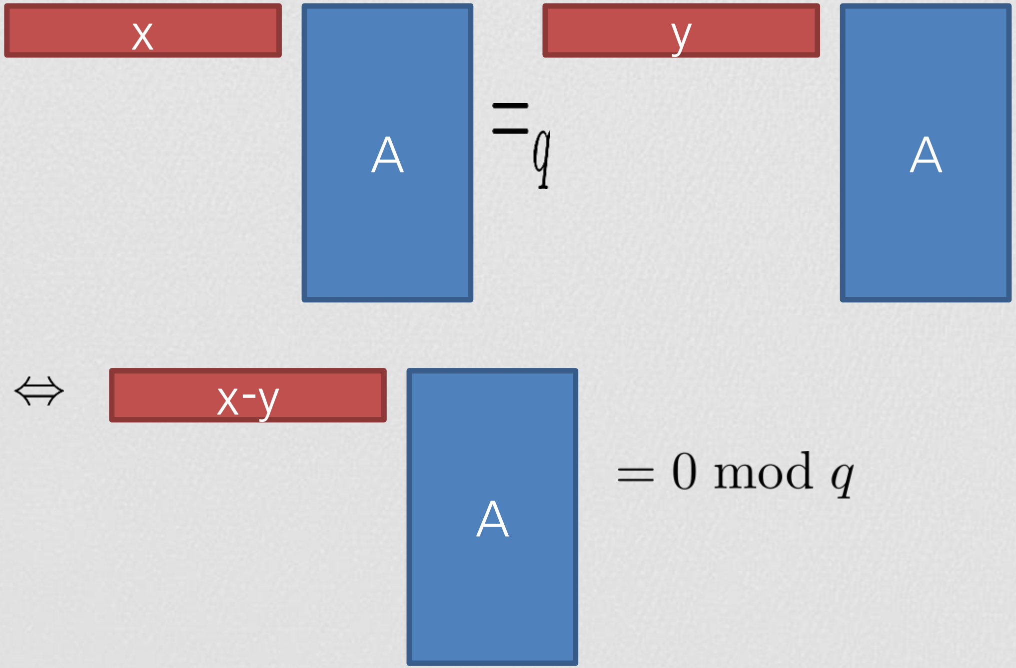
$f(x) =$

$\bmod q$

격자기반 암호 CRHF

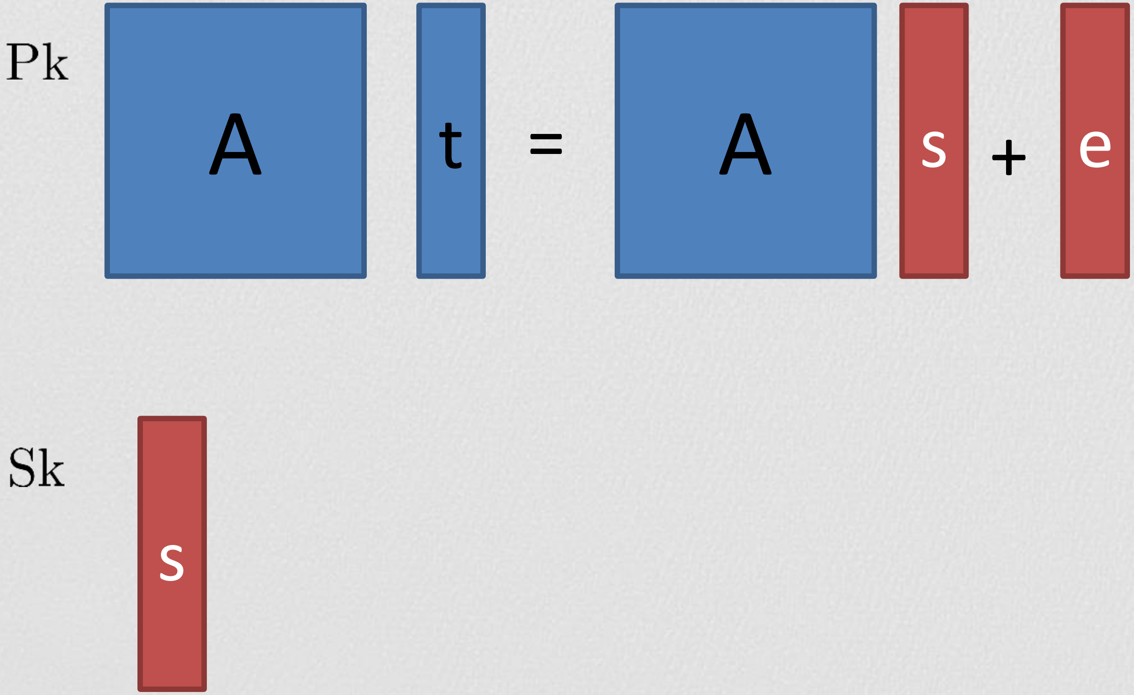
- 충돌쌍을 찾기 위해서…

$$f(x) = f(y) \Leftrightarrow$$



격자기반 암호 PKE

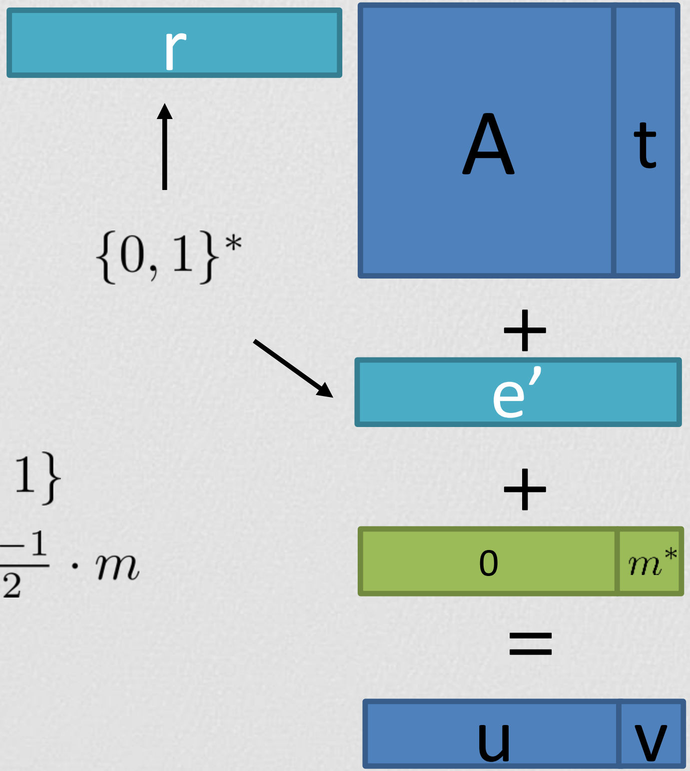
- LWE 기반 공개키 암호



격자기반 암호 PKE

- LWE 기반 공개키 암호

Enc(m)=

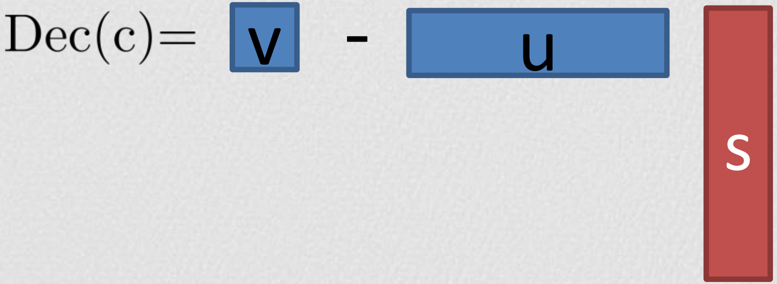


$m \in \{0,1\}$

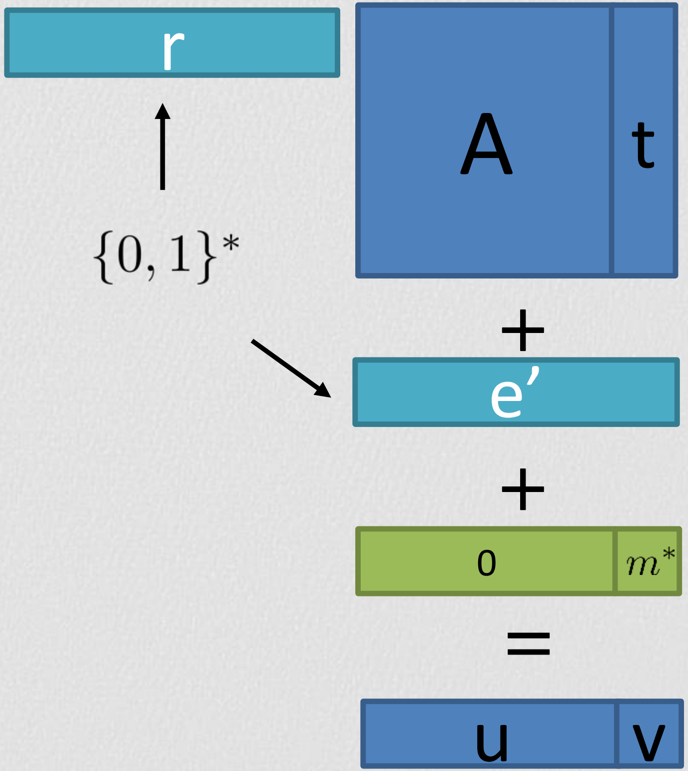
$m^* = \frac{q-1}{2} \cdot m$

격자기반 암호 PKE

- LWE 기반 공개키 암호

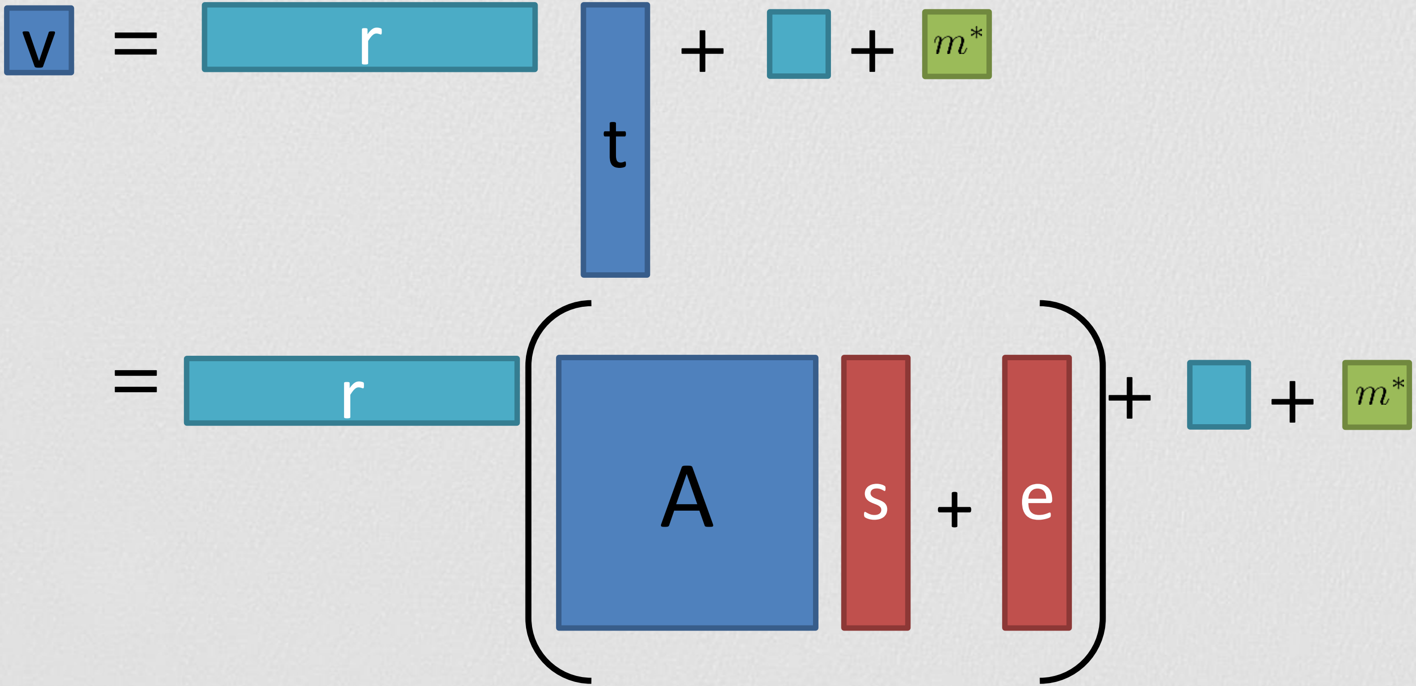


$$= \begin{cases} 0 & \text{if} \approx 0 \\ 1 & \text{if} \approx \frac{q-1}{2} \end{cases}$$



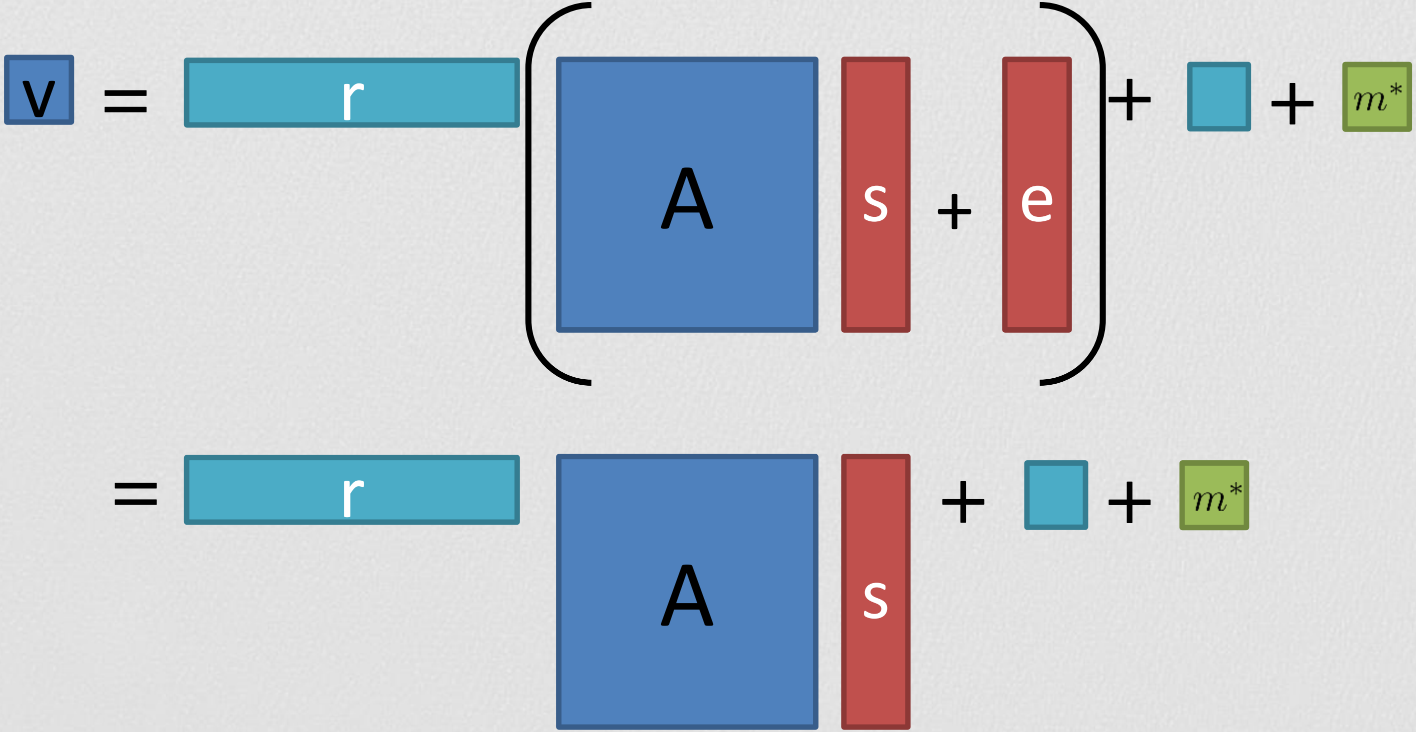
격자기반 암호 PKE

- LWE 기반 공개키 암호



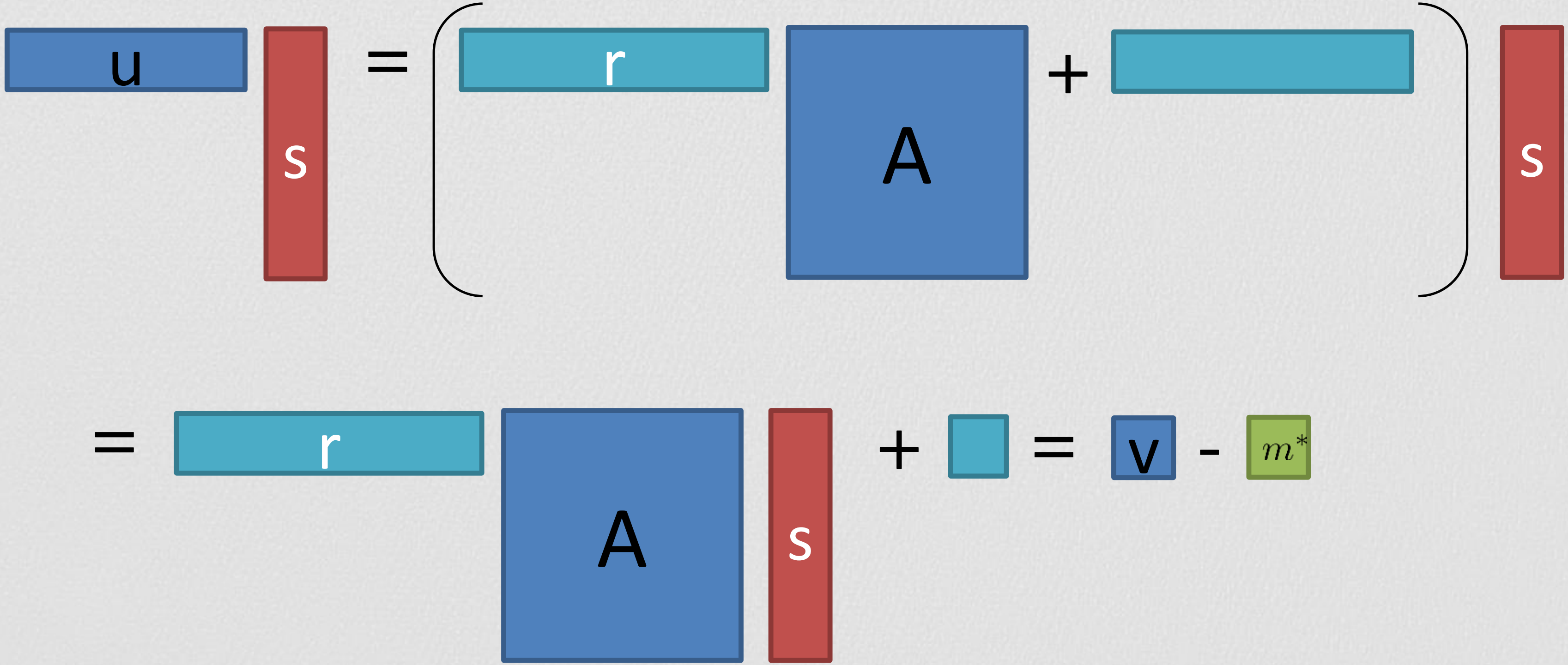
격자기반 암호 PKE

- LWE 기반 공개키 암호



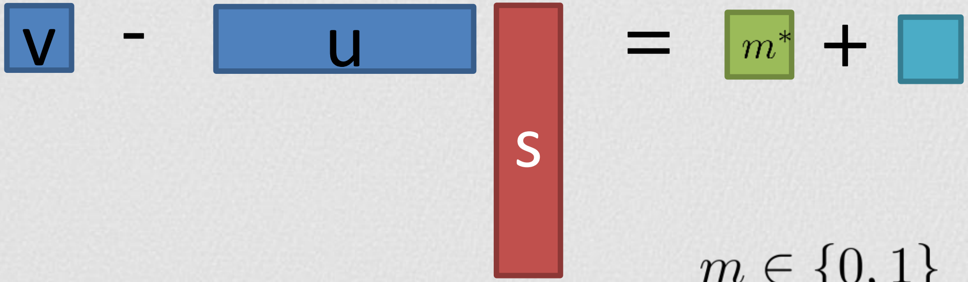
격자기반 암호 PKE

- LWE 기반 공개키 암호



격자기반 암호 PKE

- LWE 기반 공개키 암호



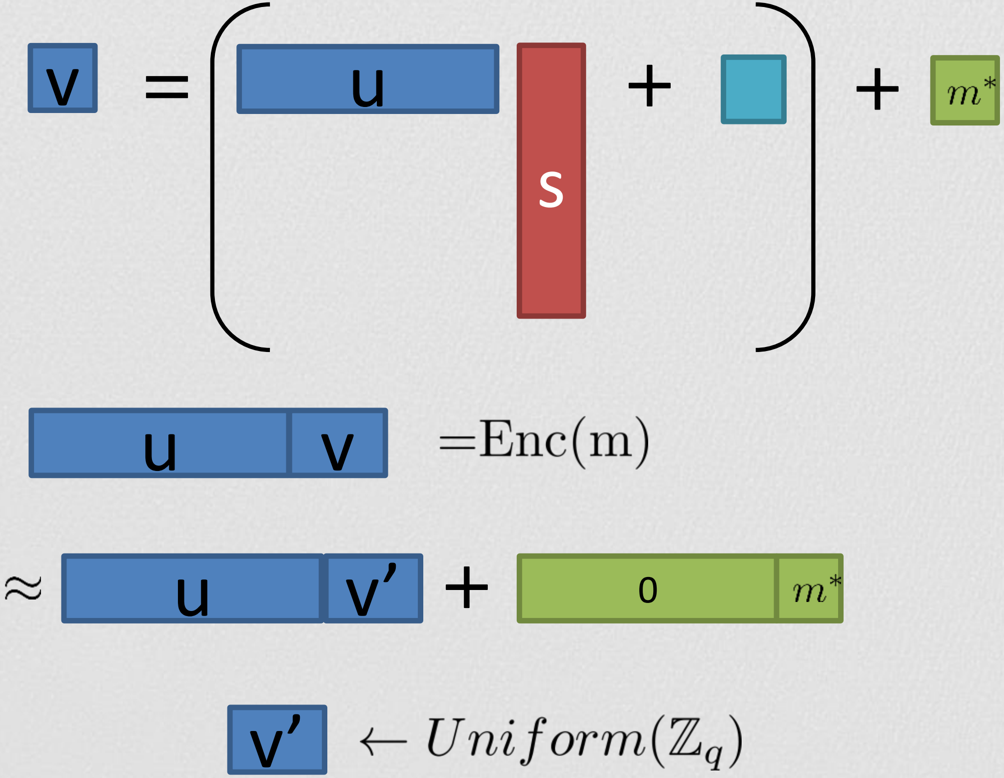
$$m \in \{0, 1\}$$

$$m^* = \frac{q-1}{2} \cdot m$$

$$= \begin{cases} 0 & \text{if} \approx 0 \\ 1 & \text{if} \approx \frac{q-1}{2} \end{cases}$$

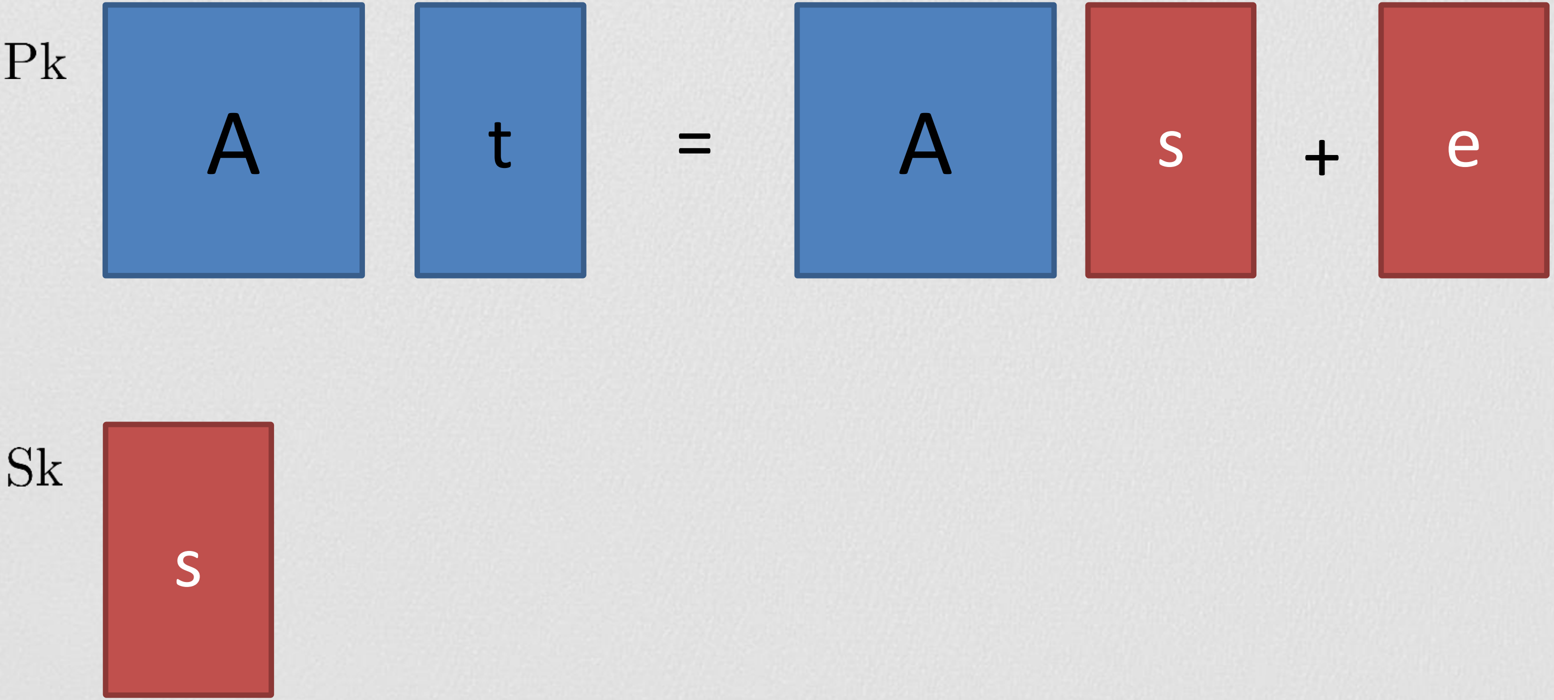
격자기반 암호 PKE

- Security



격자기반 암호 PKE

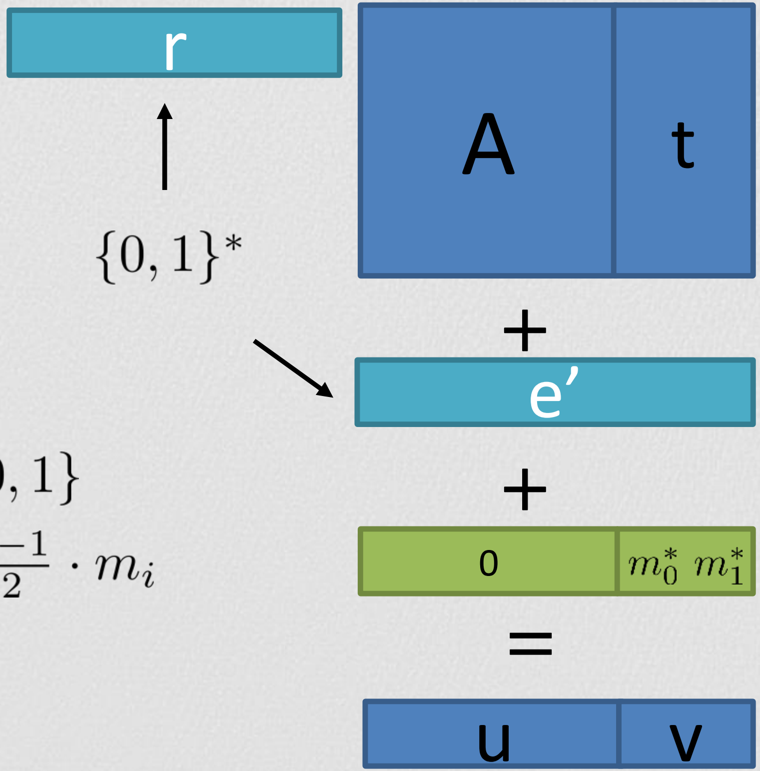
- LWE 기반 공개키 암호 (More bits)



격자기반 암호 PKE

- LWE 기반 공개키 암호

$\mathrm{Enc(m)}=$



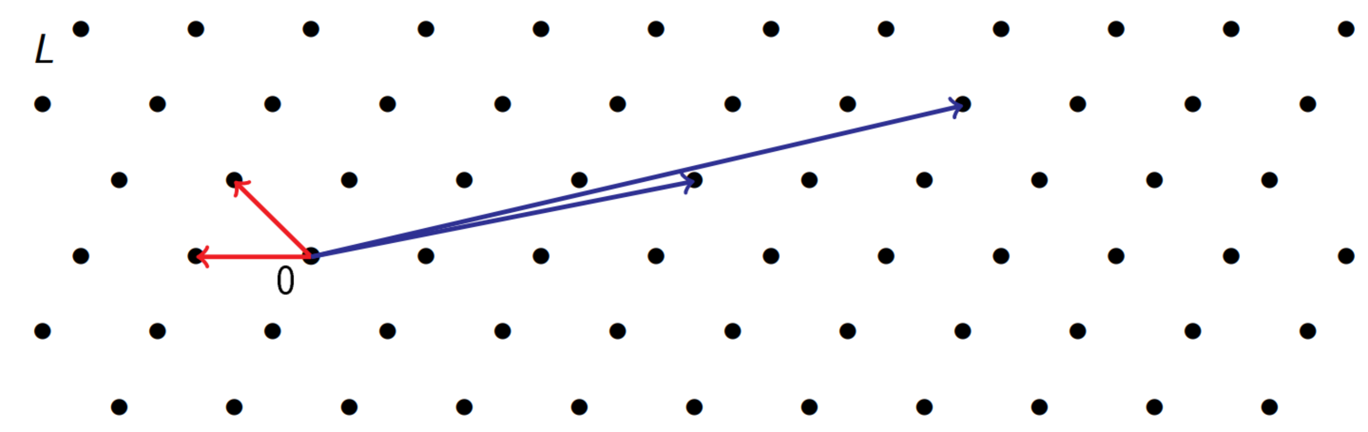
$m_i \in \{0,1\}$

$m_i^* = \frac{q-1}{2} \cdot m_i$

4

대수적 격자 소개

격자(lattices)

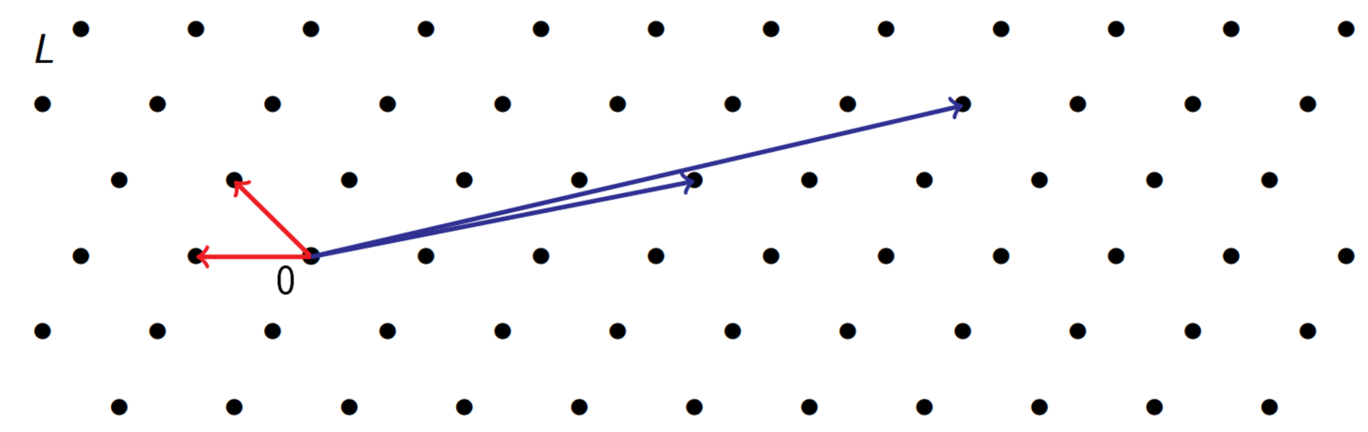


$$L = \mathcal{L}(B) = \langle B \rangle = \{Bx \mid x \in \mathbb{Z}^n\}$$

$B \in GL_n(\mathbb{Z})$: Basis matrix

n : rank

격자(lattices)



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

$B \in GL_n(\mathbb{Z})$: Basis matrix

n : rank

The Ring

$R = \mathbb{Z}[X]/\langle X^2 + 1 \rangle$

$r = r_0 + r_1 \cdot X \in R$ can be seen as

- (Polynomial) $r_0 + r_1 \cdot X$
- (Vector) (r_0, r_1)
- (Vector) $(r_0 + r_1 \cdot i, r_0 - r_1 \cdot i)$, $i = \sqrt{-1}$

The Ring

$R = \mathbb{Z}[X]/\langle X^2 + 1 \rangle$

$r, s \in R$

Operations

- $(+)$: $r_0 + r_1 \cdot X \; + \; s_0 + s_1 \cdot X$

  $$= (r_0 + s_0) + (r_1 + s_1) \cdot X$$

- $(\times)$: $r_0 + r_1 \cdot X \; \times \; s_0 + s_1 \cdot X$

  $$= (r_0 s_0 - r_1 s_1) + (r_0 s_1 + s_0 r_1) \cdot X$$

The Ring

$R = \mathbb{Z}[X]/\langle X^4 + 1\rangle$

$r = r_0 + r_1 \cdot X + r_2 \cdot X^2 + r_3 \cdot X^3 \in R$ can be seen as

- (Polynomial) $r_0 + r_1 \cdot X + r_2 \cdot X^2 + r_3 \cdot X^3$
- (Vector) (r_0, r_1, r_2, r_3)

The Ring

$R = \mathbb{Z}[X]/\langle X^4 + 1\rangle$

$r, s \in R$

Operations

- $(+)$: $r_0 + r_1 \cdot X + r_2 \cdot X^2 + r_3 \cdot X^3 \; + \; s_0 + s_1 \cdot X + s_2 \cdot X^2 + s_3 \cdot X^3$

  $= (r_0 + s_0) + (r_1 + s_1) \cdot X + (r_2 + s_2) \cdot X^2 + (r_3 + s_3) \cdot X^3$

- $(\times)$: $r_0 + r_1 \cdot X + r_2 \cdot X^2 + r_3 \cdot X^3 \; \times \; s_0 + s_1 \cdot X + s_2 \cdot X^2 + s_3 \cdot X^3$

  $=????$

Ring operation Example

$$
\begin{aligned}
& (X^3 + 7X^2 + 1) \times (9X^2 + 7) = 9X^5 + 63X^4 + 9X^2 + X^3 + 7X^2 + 1 \\
= \quad & 9X^5 + 63X^4 + X^3 + 16X^2 + 1 \\
= \quad & 9X^5 + 63X^4 + X^3 + 16X^2 + 1 - (X^4 + 1) \cdot (9X + 63) \\
= \quad & X^3 + 16X^2 - 9X - 62
\end{aligned}
$$

R: $+, \times$ 가능 $\div$??

Ring division

$$\mathbb{Z}_q = \mathbb{Z}/\langle q\mathbb{Z}\rangle$$

$$a^{-1} \in \mathbb{Z} \text{ s.t } \ a \cdot a^{-1} = 1 \bmod q\mathbb{Z}$$

$$\Leftrightarrow a \cdot a^{-1} + q \cdot c = 1 \quad \Leftarrow \text{G.C.D(a,q)}$$

$$R_q = R/\langle qR\rangle$$

$$a^{-1} \in \mathbb{R} \text{ s.t } \ a \cdot a^{-1} = 1 \bmod qR$$

$$\Leftrightarrow a \cdot a^{-1} + q \cdot c = 1 \quad \Leftarrow \text{G.C.D(a,q)????}$$

Ring division

$$R_q = R/\langle qR \rangle \quad R = \mathbb{Z}[X]/\langle X^2+1 \rangle$$

$$a \cdot a^{-1} + q \cdot c = 1$$

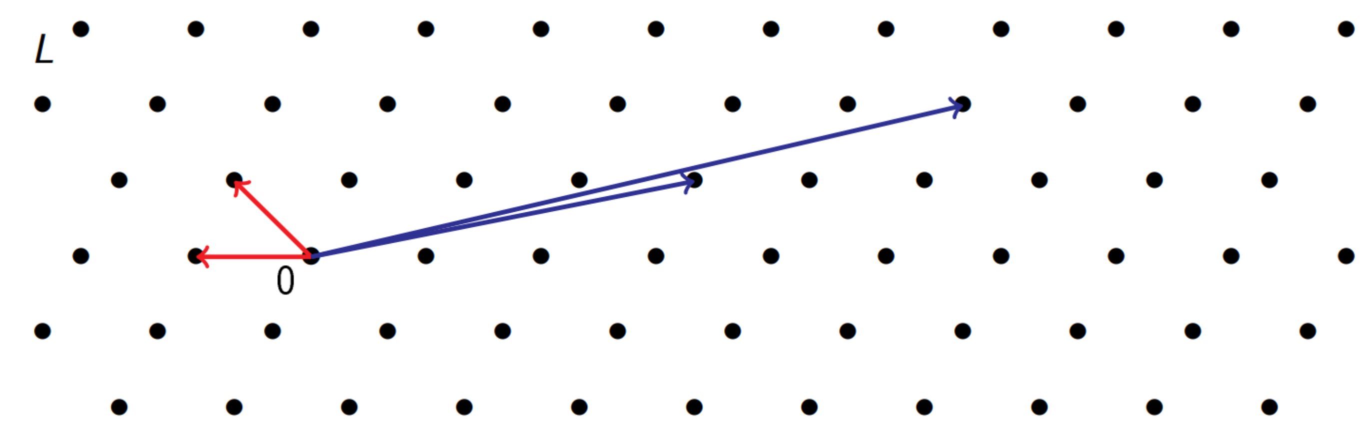
$$\begin{aligned} a &= a_0 + a_1 X \\ aX &= a_0 X + a_1 X^2 \\ &= -a_1 + a_0 X \end{aligned}$$

$$\Rightarrow a_0 \cdot a - a_1 \cdot aX = a_0^2 + a_1^2$$

$$\Rightarrow s \cdot (a_0^2 + a_1^2) + q \cdot c = 1$$

$$\Rightarrow a^{-1} = s \cdot (a_0 - a_1 X)$$

대수적 격자(Algebraic lattices)



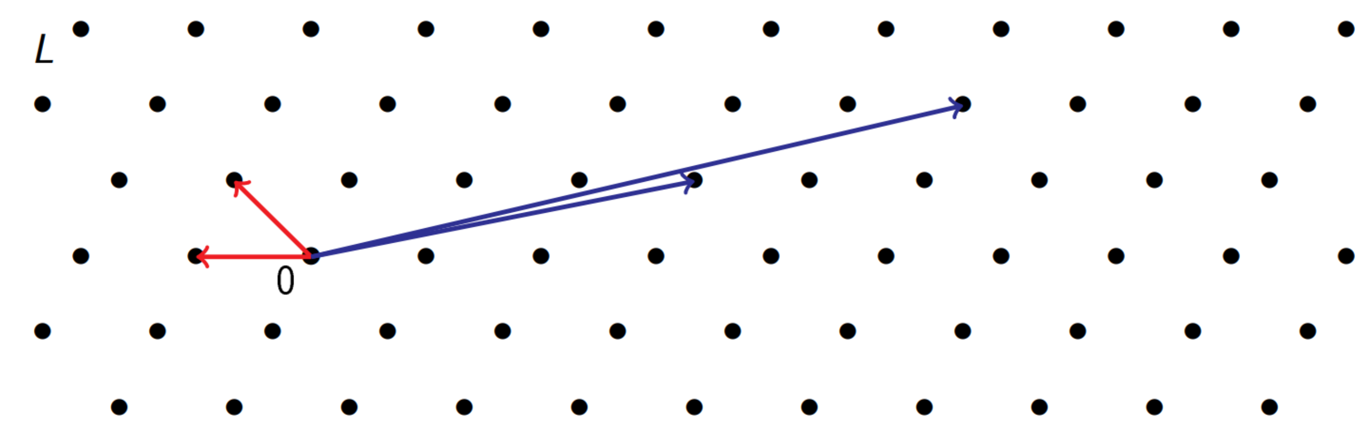
$$L = \mathcal{L}(B) = \langle B \rangle = \{Bx \mid x \in R^n\} \quad R = \mathbb{Z}[X]/\langle X^m + 1 \rangle$$

$B \in GL_n(R)$: Basis matrix

n : rank

m: extension degree

대수적 격자(Algebraic lattices)



$$L = \mathcal{L}(B) = \langle B \rangle = \{Bx \mid x \in R^1\}$$

$B = \langle b \rangle \in GL_1(R)$: Basis matrix

아이디얼 격자 $(Ideal\ lattice)$

아이디얼 격자

$$B = \langle b \rangle = \{b \cdot r \mid r \in R\} = \sum_{i=0}^{n-1} b \cdot X^i$$

$\text{SVP on } B$

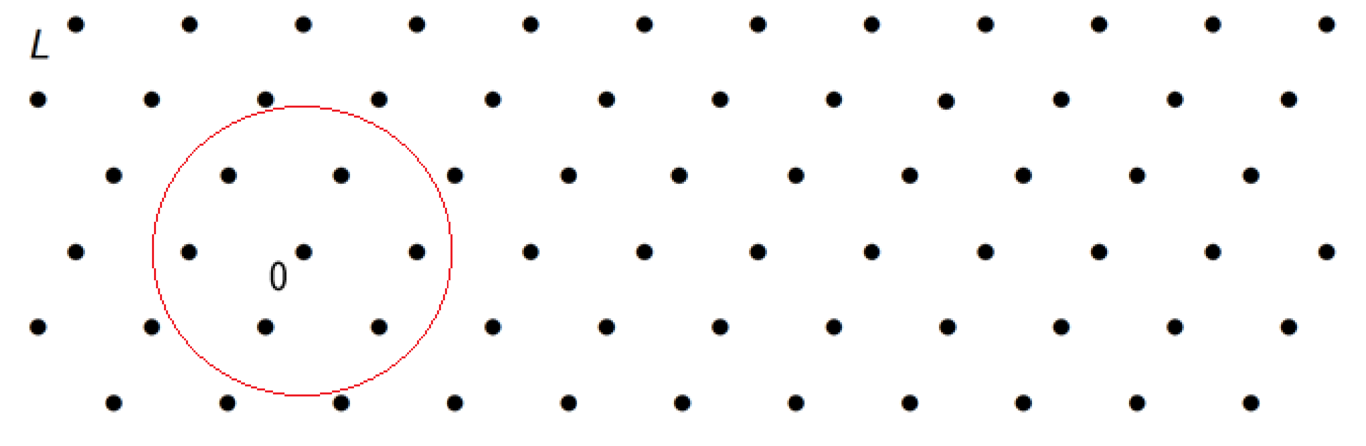
최소 길이를 갖는 b의 배수를 찾아라

아이디얼 격자의 길이란?

$$r \Leftrightarrow (r_0, r_1, r_2, r_3)$$

$$\|r\| = \sqrt{r_0^2 + r_1^2 + r_2^2 + r_3^2}$$

아이디얼 격자의 짧은 원소



ideal SVP: Ideal shortest vector problem

Input: $B = \langle b \rangle$

Output: $a = a \cdot b \in \langle b \rangle$

아이디얼 격자의 짧은 원소

$R = \mathbb{Z}[X]\langle X^4 + 1\rangle$

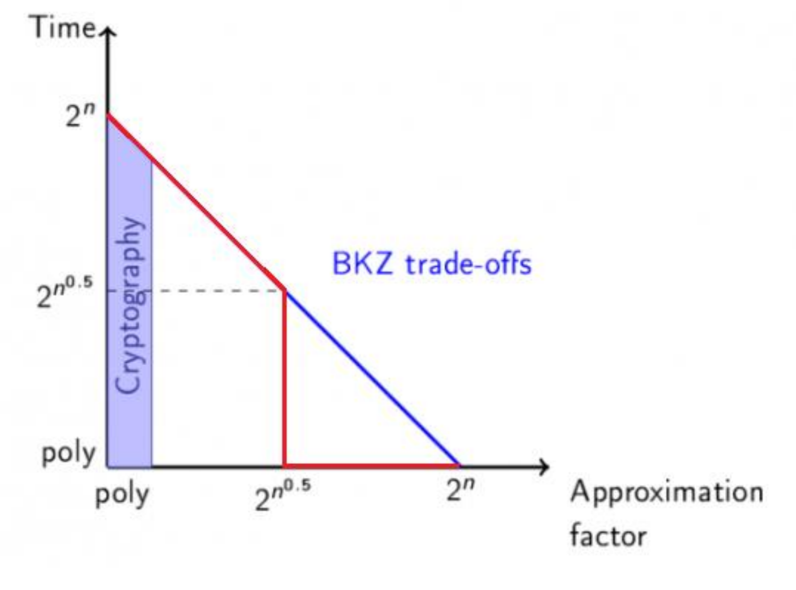
Input: $B = \langle X^3 + 2X^2 + 2X + 1\rangle$

$\|X^3 + 2X^2 + 2X + 1\| = \sqrt{10}$

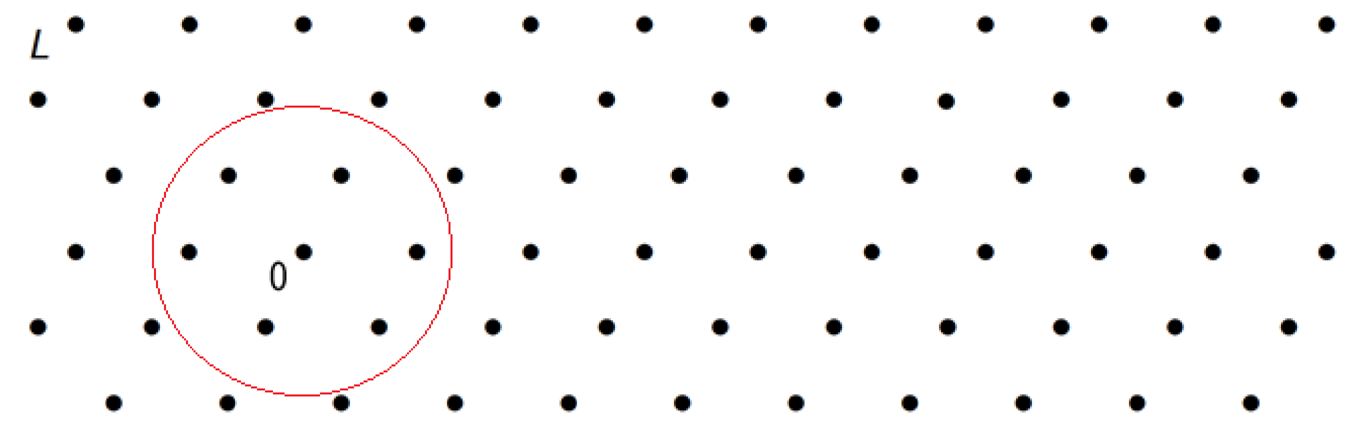
$\|(X^3 + 2X^3 + 2X + 1) \cdot (-X^3 - X^2 + 1)\|$
$= \|X + 1\| = \sqrt{2}$

Ideal SVP in practice

현재 ideal SVP는 얼마나 풀 수 있을까?



대수적 격자의 짧은 벡터



Module SVP: Module shortest vector problem

Input: $B \in R^{m \times m}$ $m \leq 10$

Output: 가장 짧은 길이의 벡터

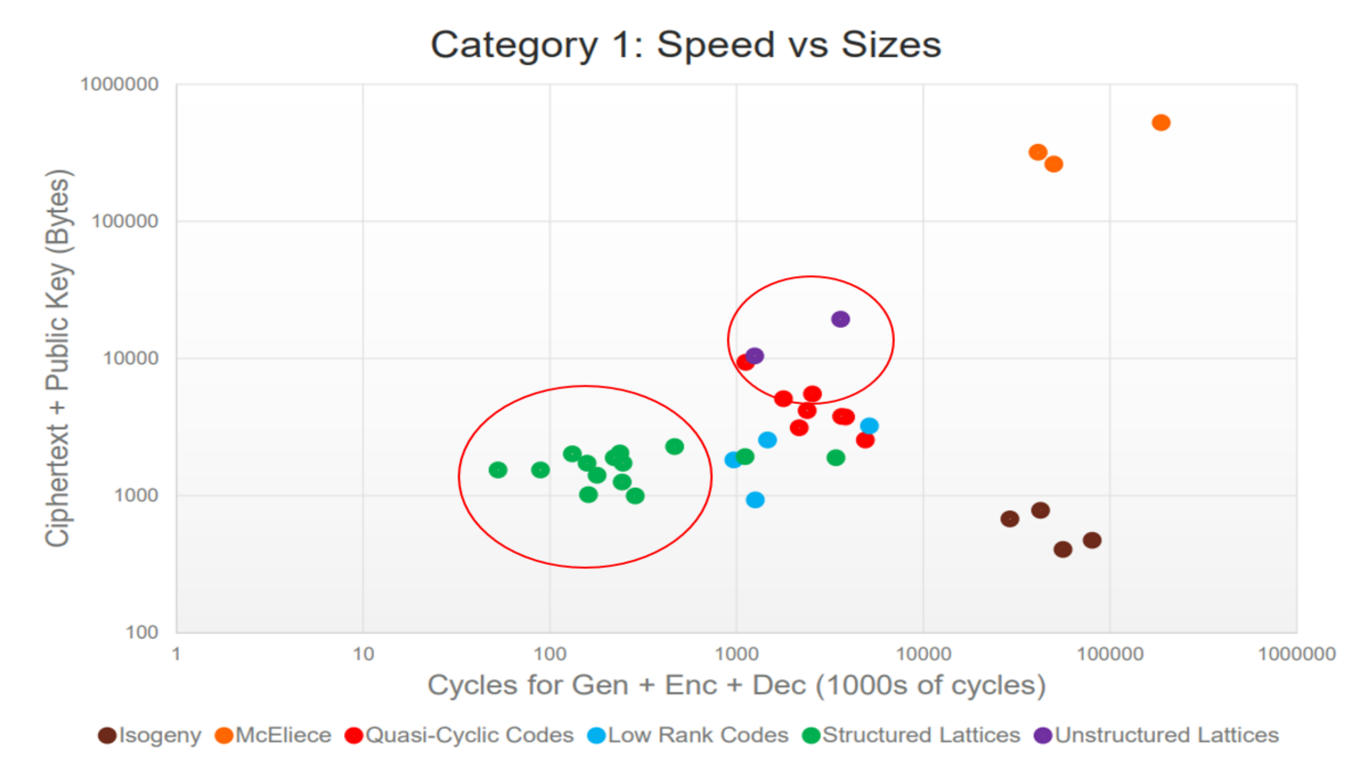
Why algebraic lattice?

- 저장 공간에서서의 장점
  -rank n 격자를 표현하기 위해서 1벡터면 충분
  $$B = \langle b \rangle = \{b \cdot r \mid r \in R\} = \sum_{i=0}^{n-1} b \cdot X^i$$

- 대수적 구조
  -FFT(fast fourier transformation)이용가능

$\Rightarrow$암호의 저장공간과 동작시간을 고속화시켜줌

Why algebraic lattice?



Data from NIST

RLWE (Ring-Learning with errors) 문제

$q \in \mathbb{Z},\ R_q := R/qR = \mathbb{Z}_q[X]/\langle X^n + 1\rangle$

Given $\boxed{a}$ and $\boxed{b} = \boxed{a}\,\boxed{s} \bmod q$

Recover s

$\boxed{a} \leftarrow Uniform(R_q)$ $\boxed{s} \leftarrow N(0, \sigma)^n$

Easy!! ($\div$ is possible)

RLWE (Ring-Learning with errors) 문제

$q \in \mathbb{Z},\ R_q := R/qR = \mathbb{Z}_q[X]/\langle X^n + 1\rangle$

Given $\boxed{a}$ and $\boxed{b} = \boxed{a}\,\boxed{s} + \boxed{e} \mod q$

Recover s and e

$\boxed{a} \leftarrow Uniform(R_q) \quad \boxed{s}\ \boxed{e} \leftarrow N(0, \sigma)^n$

Still hard

RLWE (Ring-Learning with errors) 문제

$$q \in \mathbb{Z},\ R_q := R/qR = \mathbb{Z}_q[X]/\langle X^n + 1 \rangle$$

Given A and $t = A s + e$

Recover s and e

$A \leftarrow Uniform(R_q^{m \times m})$ $\quad$ s e $\leftarrow N(0, \sigma)^m$

Still hard

NTRU 문제

$q \in \mathbb{Z},\ R_q := R/qR = \mathbb{Z}_q[X]/\langle X^n + 1\rangle$

Given $\boxed{h}$ and $\boxed{h} = \dfrac{\boxed{g}}{\boxed{f}} \bmod q$

Recover g and f

$\boxed{g}\ \boxed{f} \leftarrow \{-1, 0, 1\}^n$

Also hard

$$q \in \mathbb{Z},\ \mathbb{Z}_q$$
$$f = 3, g = 2 \text{ and } q = 1031$$
$$h = g/f = -343 \bmod q$$

격자와 아이디얼 격자 기반 문제 비교

	격자	아이디얼 격자
SVP	NP hard	?
SIVP	NP hard	?
uSVP	NP hard	?
BDD	NP hard	?
NTRU	Easy	?
LWE	NP hard	?