* $\mathbb{Z}_q$ 는 $(-\frac{q}{2}, \frac{q}{2}]$ 라고 하기도 함 $(0, q]$ 로 하기도 하고, 여러가지 원소.

* λ = 정수인 security parameter. (공격자의 능력) (ex) 2^{80}, 2^{100}, 2^{200} 컴퓨터에게 클수록 공격자가 강함

=> 논문에서는 80으로 가정했지만 요즘에는 128 정도로 잡음!

* field 체 => $R(R, +, \times)$: inverse 덧셈, 항등 ㅇ
$F(R, +, \times)$: inverse " " + inverse => ∴ 역원존재 가능

↳ $\mathbb{Q}[x]/\Phi_m(x)$ 로 정의가능 => 소수를 다루겠다.

$\mathbb{R}[x]/\Phi_m(x)$ ..

* 다항식의 계수들을 벡터로도 사용.

CRT^{-1}, CRT 공부.
↔
↳ Coeffi, evalu

* Canonical Embedding Norm => FFT (evaluation point 를 벡터로) ← 오늘 내용

=> primitive root 를 넣은 값들 최댓값 ($\mathbb{Q}[x]/\Phi_m(x)$ 에 대입)

↳ evaluate 한 $f(3_1), f(3_2), \cdots f(3_{\phi(m)})$ 중 최대값 (상수)

* CRT $f(x) = \sum_{i=0}^{n-1} a_i x^i$ // $f(3^i)/_{i \in \mathbb{Z}_m^*}$

$i=1$ |
$f(3_1) = a_0 + a_1 3_1^1 + a_2 3_1^2 + a_3 3_1^3 + \cdots$
$f(3_2) = a_0 + a_1 3_2^1 + a_2 3_2^2 + a_3 3_2^3 + \cdots$
$f(3_{\phi(m)}) = a_0 + a_1 3_{\phi(m)}^1 + a_2 3_{\phi(m)}^2 + \cdots$

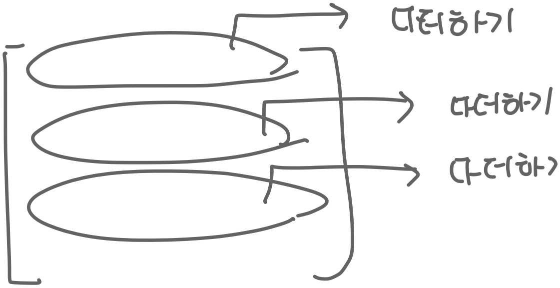
CRT$_M$, CRT$_M^{-1}$ 로 왔다갔다함.

Coeff, evaluate 바꿀때 이렇게 사용

=> CRT$_M$ = 오른쪽 행렬

evaluation ↓ Coeffi ↓ evaluate

$$\begin{bmatrix} 1 & 3_1 & 3_1^2 & \cdots \\ 1 & 3_2 & 3_2^2 & \cdots \\ \vdots & & & \\ 1 & 3_m & & \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{bmatrix} = \begin{bmatrix} f(3_1) \\ f(3_2) \\ \vdots \\ f(3_{\phi(m)}) \end{bmatrix}$$



다 더한 값들 중 가장 큰 값

$= \|U\|_\infty = \left\{ \sum_{j=0}^{M} |u_{ij}| \right\}$

행렬 CRT의 원소 i,j로 표현

- **Gaussian Distributions and RLWE Problem**

  ↳ 이 page 에서

원래 $\mathbb{Z}[x]/\Phi_M(x)$ 에서 ← encoding — $\mathbb{Z}[x]/\zeta_1, \zeta_2 \cdots$ → decoding

$$H = \{ z = (z_j)_{j \in \mathbb{Z}_M^*} \in \mathbb{C}^N : z_j = \overline{z_{-j}} \quad \forall j \in \mathbb{Z}_M^* \}$$

$$U = \begin{pmatrix} \frac{1}{\sqrt{2}} I & \frac{i}{\sqrt{2}} J \\ \frac{1}{\sqrt{2}} J & \frac{-i}{\sqrt{2}} I \end{pmatrix}$$

(I = identity matrix size of $\frac{N}{2}$, J = reversal matrix) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$\mathbb{C}[x]/\Phi_m(x) \longmapsto \mathbb{C}^{M^*}$ ← encoding ($\times$CRT^{-1}), → decoding ($\times$CRT)

plaintext space

↳ plaintext vector (저장위해, 연산도↑, eval 해줌 FFT도 같이)

$f(x) \longmapsto (f(\zeta_1), f(\zeta_2), \cdots,)$

$\mathbb{R}[x]/\Phi_m[x]$

$f(M) = M^*$

$f(x) \longmapsto (f(\zeta_1), f(\zeta_2), \cdots f(\zeta_{\frac{M^*}{2}})), \overline{f(\zeta_1)}, \overline{f(\zeta_2)}, \cdots \overline{f(\zeta_{\frac{M^*}{2}})}$

$f(\zeta_1) = 3+2i$, $f(\zeta_2) = 2-5i$, $3-2i$, $2+5i$ (반대방향이)

$(a+bi, c+di) \longmapsto (a+bi, c+di, a-bi, c-di)$

=> Msg vector → Msg space로 하는데 그 결과를 「리얼」 해서 message로 쓴다.

$\zeta_1 = e^{\frac{2\pi i}{N}}$ 이라는 특별한 조건에서는 $(\zeta^M) = 1$ 이 되어 다시 돈다.

↳ 가장 큰 Space 에서 생각한다고 복소수를 표현

⇒ 공간 다쓰면 복소수 공간 가지는데, 정수로 할려면 $\mathbb{C}$가 아니어야 하는데

⟷ 켤레 성질이다

(⇒) $f(x) \in \mathbb{R}$ 이면 $(m_1, m_2, \dots, m_{\frac{N}{2}}, \bar{m}_1, \bar{m}_2, \dots, m_N)$

(⇐) $(x_1, x_2, \dots, x_{\frac{N}{2}}, \bar{x}_1, \bar{x}_2, \dots)$ → Encoding 하면 실수 계수를 가진다.

∴ <u>Msg 절반만 쓴다</u> (conjugate 이기 때문) ⇒ 그리고 실수 ⇒ 정수로 바꾼다.

위의 식이다 (conjugate 하는식)

잔데메이리와 이어짐

$$\begin{pmatrix} 1 & 0 & 0 & i \\ 0 & 1 & i & 0 \\ 0 & 1 & -i & 0 \\ 1 & 0 & 0 & -i \end{pmatrix} \begin{pmatrix} a \\ c \\ d \\ b \end{pmatrix} = \begin{pmatrix} a+bi \\ c+di \\ c-di \\ a-bi \end{pmatrix}$$

conjugate
conjugate

Encoding

Step 1 ⇒ $(m_1, m_2, \dots, m_{\frac{N}{2}}) \in \mathbb{C}^{\frac{N}{2}}$

Step 2 ⇒ $(m_1, \dots, m_{\frac{N}{2}}, \bar{m}_1, \bar{m}_2, \dots, \bar{m}_{\frac{N}{2}}) \in \mathbb{C}^N$

↳ 위의 ( ) 함수로 확장 켤레 다 찾음

Step 3 ⇒ $CRT^{-1} \times m_x$ = 계수들 다 찾음

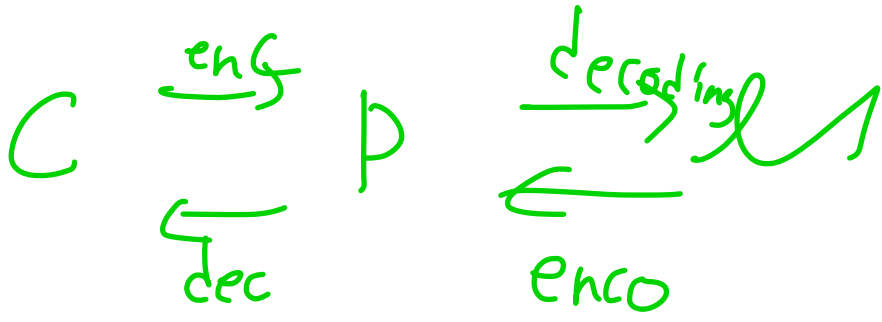
↓ $\begin{bmatrix} a \\ \vdots \end{bmatrix} \in \mathbb{R}$

↳ π^{-1} = 확장할 켤레 찾게

σ = CRT

⇒ 서로는 Enco, Deco 제안, Canonical로 이용해서,

그 자체로 활용하니 (Cano) 그게 안되고, 실수 계수 위해 (켤레조건 만들어줌)



$P \simeq \ell 1$ isomorphism

$a \quad (a_1 \ a_2 \ a_3)$

$*_b \qquad *$

$(b_1 \ b_2 \ b_3)$

2개정보를 다포함하고 있다.

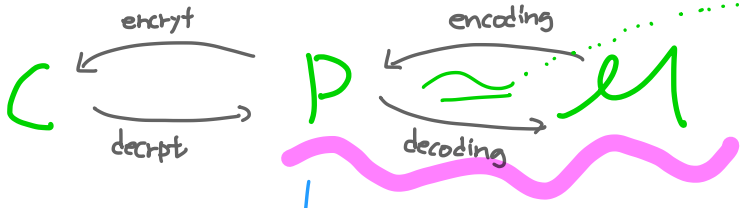
$M=8, \quad \Phi_8(x) = x^4+1$

$\Rightarrow (1+2i, \ 6-5i, \ 6+6i, \ 1-2i)$

↓ 6-1 해줄

$m(x) \leftarrow \mathbb{R}[x]$ ∴ M의 2개 encoding 함

=> 랩실 끝나고 총정리



P와 M는 isomorphism 성질로 만들어

$a \times b = (a_1, a_2, a_3, \cdots) \times (b_1, b_2, b_3, \cdots) = \cdots$

$\langle P \rangle$ $\langle M \rangle$ 성립하는 공간

↳ 이부분을 기존 BGV는

$\mathbb{Z}_q/\Phi_m(x)$ ⇄ (encoding / decoding) $\mathbb{Z}_q/f_1 \times f_2 \times \cdots$

$\Phi_m(x)$ = 여러개의 f로 표현해서 사용!

CKKS는 다른 새로운 방법으로 소수까지 다룰수 있게함.

주제

=> Canonical embed 방법을 사용했으나, 그렇게 할경우 복소수가 plain text에 포함되기 때문에 이를 해결하기 위해 extension (T)를 사용해 씨들을 원래 형태로 만들어 CRT를 통해 plain text (여러 메시지 정보를 담을 평문 만듦)

* 체 :

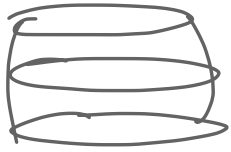
	+	×
Ring $(R,+,\times)$:	Inverse	닫힘, 항등
Field $(R,+,\times)$:	Inverse	〃 + Inverse

* 상식 + : λ (sequrity parameter) (공격 자의 능력 계량)

↳ 과거에는 80정도로 했으나 quantum으로 보통은 128로 잡는다. (2^{80}, 2^{128} 만큼 공격능력)

- Canonical Embedded Norm. 과 CRT matrix

↳ 행렬 에서 가로로 더한 값들 가장 큰것



$$\Rightarrow \|V\|_\infty = \left\{ \sum_{j=0}^{N-1} \|a_{ij}\| \right\}$$

CRT matrix 는

$f(x) = \sum_{i=0}^{m} a_i x^i$ 로 만든다 이는 행렬로 표현가능

$$\begin{bmatrix} 1 & 3_1 & 3_1^2 & \cdots & 3_1^{n-1} \\ 1 & 3_2 & 3_2^2 & \cdots & 3_2^{n-1} \\ \vdots & & & & \\ 1 & & & & 3_{n-1}^{m} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} f(3_1) \\ f(3_2) \\ \vdots \\ f(3_{gen}) \end{bmatrix}$$

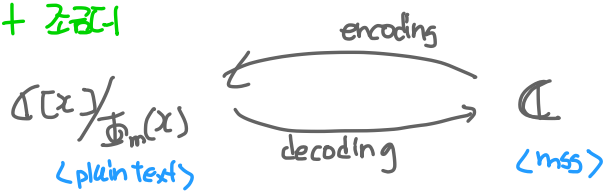
↳ CRT (6) — Coefficient (plain text 계수) — evaluation value (msg 의 값)

즉 FFT 에서 계수 표현 ⟷ evaluate 점 표현

왔다리 갔다리 하여 $n^2 \rightarrow n \lg n$ 으로 줄어든것처럼

plain 공간 ⟷ 시 공간 왔다리 갔다리 한다 이를 encoding, decoding 이라고 한다!

+ 고려사항



↳ 고등하면 plain text 계수 복소수가 나와 msg 에서 결례 만족 만들어서 CRT 행열 곱하면 이는 유리수 계수를 가지고, 이를 $\lfloor \cdot \rceil$ rounding 해줘서 정수 계수를 가지는 plaintext 를 만든다.

extension (켤레구하는) 행렬을 π 라고 하자

$$\begin{pmatrix} 1 & 0 & 0 & i \\ 0 & 1 & i & 0 \\ 0 & 1 & -i & 0 \\ 1 & 0 & 0 & -i \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \Rightarrow \begin{pmatrix} a+bi \\ c+di \\ c-di \\ a-bi \end{pmatrix}$$

π

$\Rightarrow$ 켤레 (conjugate) msg 들을 만들수 있다.

- Encoding Process (CKKS)

step 1 => $(m_1, m_2, \cdots, m_{\frac{N}{2}}) \in \mathbb{C}^{\frac{N}{2}}$

Step 2 => $(m_1, m_2, \cdots m_{\frac{N}{2}}, \overline{m_1}, \overline{m_2}, \cdots, \overline{m_{\frac{N}{2}}}) \in \mathbb{C}^N$

↳ π (extension) 행렬로 곱함

Step 3 => 새로운 msg X CRT => 계수

ex) 우리가 $3+2i$, $5-i$ 를 메세지로 준다.

$M=8 \Rightarrow \Phi_8(x) = x^4+1$ 이다. (즉 Mss 4개가능 인데 절반은 켤레로 써야함으로 2개 가능)

$3^i = e^{\frac{2\pi i}{8}}$ 임으로 $CTR = \begin{pmatrix} 1 & 3_1 & 3_1^2 & \cdots & 3_n^n \\ 1 & \vdots & & & \vdots \\ & & & & 3_n^n \end{pmatrix}$ 이를 알고있다.

$$\begin{pmatrix} CRT \end{pmatrix}^{-1} \begin{pmatrix} 3+2i \\ 5-i \\ 3-2i \\ 5+i \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} \Rightarrow \text{고 } f(x) \text{를 구한다.}$$

$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$ 의 계수는 실수이고,

이 $f(x)$는 2개의 메시지 $(3+2i, 5-i)$의 정보를 가지고 있다.