Homomorphic Encryption

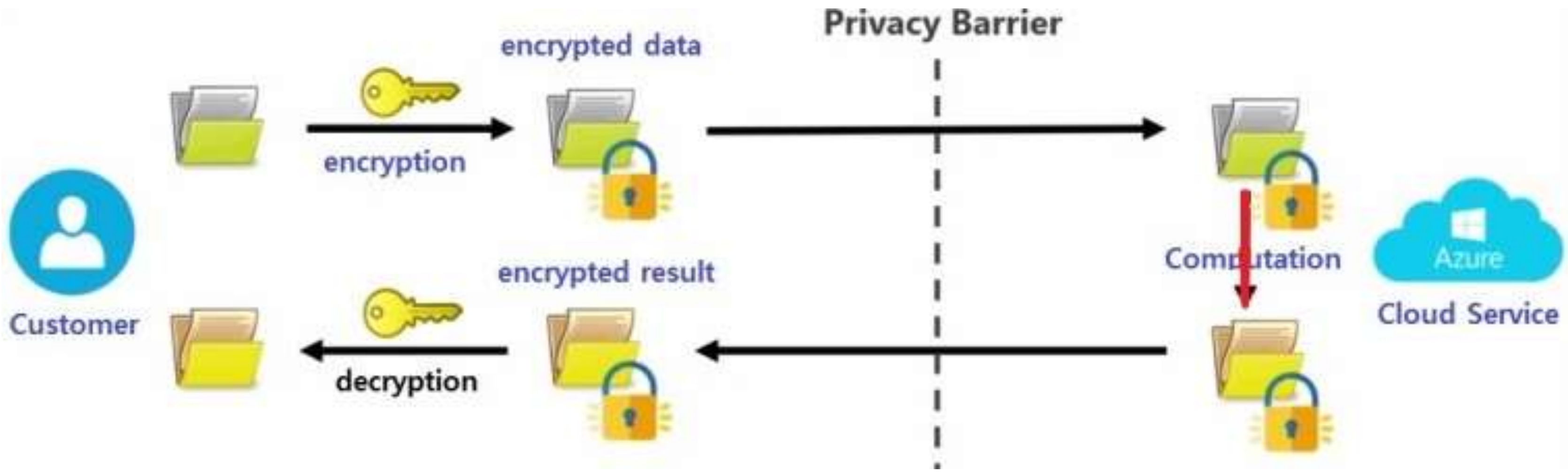
(CKKS Scheme)

2023-11-13 MIMIC Seminar

Presenter: 김지훈

Introduction

- Homomorphic Encryption (HE)는 암호화된 데이터를 복호화 없이 수학적 연산을 수행할 수 있도록 하는 cryptographic scheme
- 동형암호는 금융, 의료, 유전자 등 privacy가 중요한 데이터를 평가하는 알고리즘에 적용



HE Schemes

2세대 동형암호 (int – 정수)

- BGV [1], BFV [2]

3세대 동형암호 (bit)

- FHEW [3], TFHE [4]

4세대 동형암호 (double – 64bit 실수)

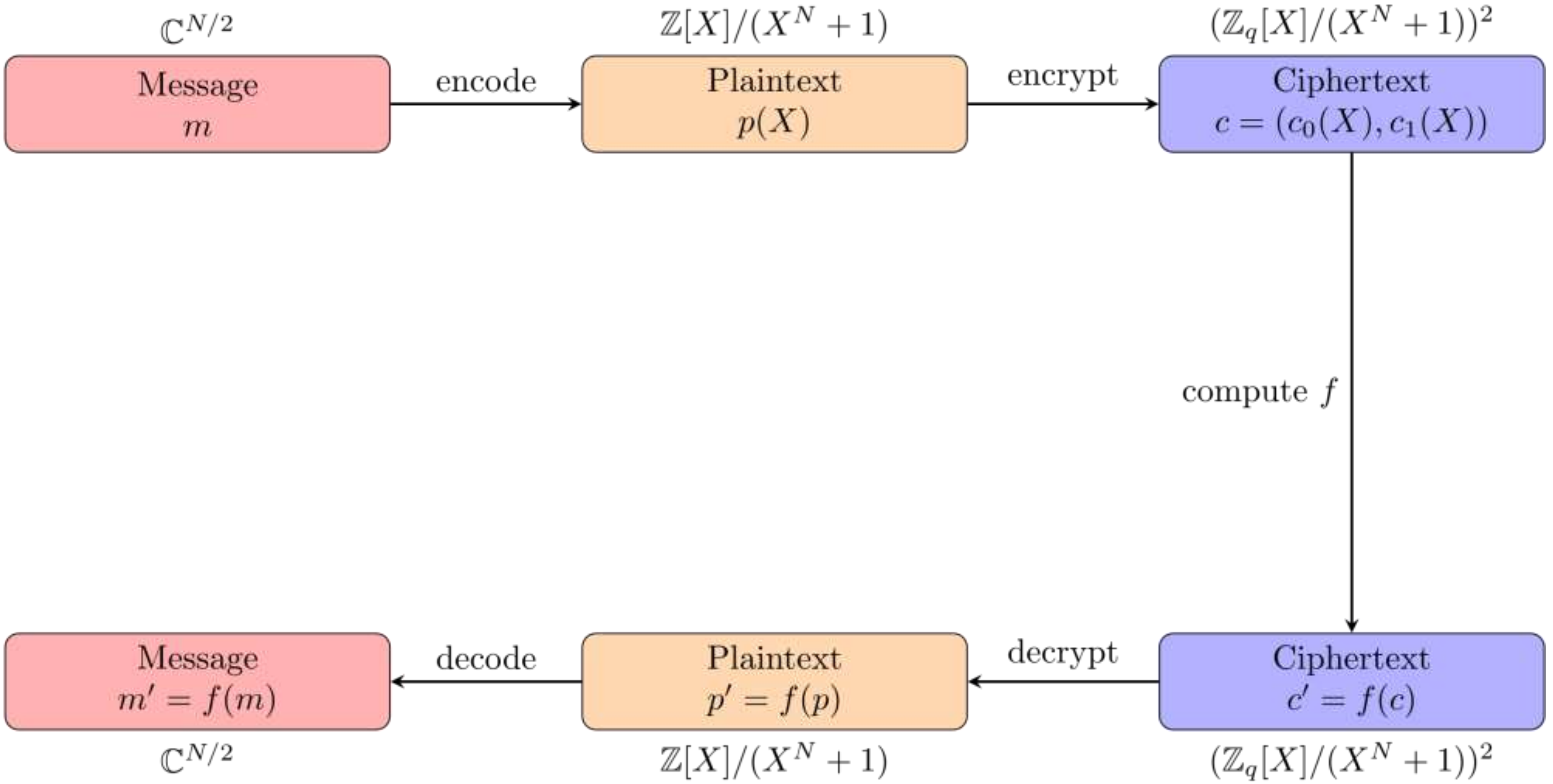
- CKKS [5] (Cheon-Kim-Kim-Song)

[1] Z. Brakerski et al., "(Leveled) fully homomorphic encryption without bootstrapping." *ITCS (2012*).
[2] J. Fan et al., "Somewhat practical fully homomorphic encryption," *Cryptology ePrint Archive* (2012).
[3] L. Ducas., "FHEW: bootstrapping homomorphic encryption in less than a second." *EuroCrypto (2015).*
[4] Chillotti, Ilaria, et al. "Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds." *AsiaCrypto (2016).*
[5] J. H. Cheon et al., "Homomorphic Encryption for Arithmetic of Approximate Numbers," *AsiaCrypto (2017).*

Open Libraries

Library	Support Schemes	Langauge	URL
IBM Helib	BGV / CKKS	C++	https://github.com/homenc/HElib
Microsoft SEAL	BFV / BGV / CKKS	C++, C#	https://github.com/microsoft/SEAL
HEAAN	CKKS	C++	https://github.com/snucrypto/HEAAN
Lattigo	BFV / BGV / CKKS	Go	https://github.com/tuneinsight/lattigo

CKKS scheme



$\mathbb{C}^{N/2}$
Message
m
encode
$\mathbb{Z}[X]/(X^N+1)$
Plaintext
$p(X)$
encrypt
$(\mathbb{Z}_q[X]/(X^N+1))^2$
Ciphertext
$c = (c_0(X), c_1(X))$
compute f
Ciphertext
$c' = f(c)$
$(\mathbb{Z}_q[X]/(X^N+1))^2$
decrypt
Plaintext
$p' = f(p)$
$\mathbb{Z}[X]/(X^N+1)$
decode
Message
$m' = f(m)$
$\mathbb{C}^{N/2}$

Background

Basic Notation

- $\mathbb{Z}_q = \{0, 1, 2, \cdots, q-1\}$
- $\mathbb{Z}_q^n = \mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q$
- $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}_q^n$라 할 때, $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = \sum_{i=0}^{n-1} a_i b_i$ (dot product, inner product)

격자 (Lattice)

계수가 $\mathbb{Z}$(정수 집합)에 속하는 linearly independent vectors $b_1, \ldots, b_n \in R^m$의 선형 결합으로 정의되는 대수적 구조를 격자(Lattice)라고 한다.

$$L = \{a_1 b_1 + \cdots + a_n b_n : a_1, \ldots, a_n \in \mathbb{Z}\}$$

여기서 $b_1, \ldots, b_n$ 은 격자 L을 생성하는 linearly independent vertors이고, L의 기저(basis)라고 불린다.

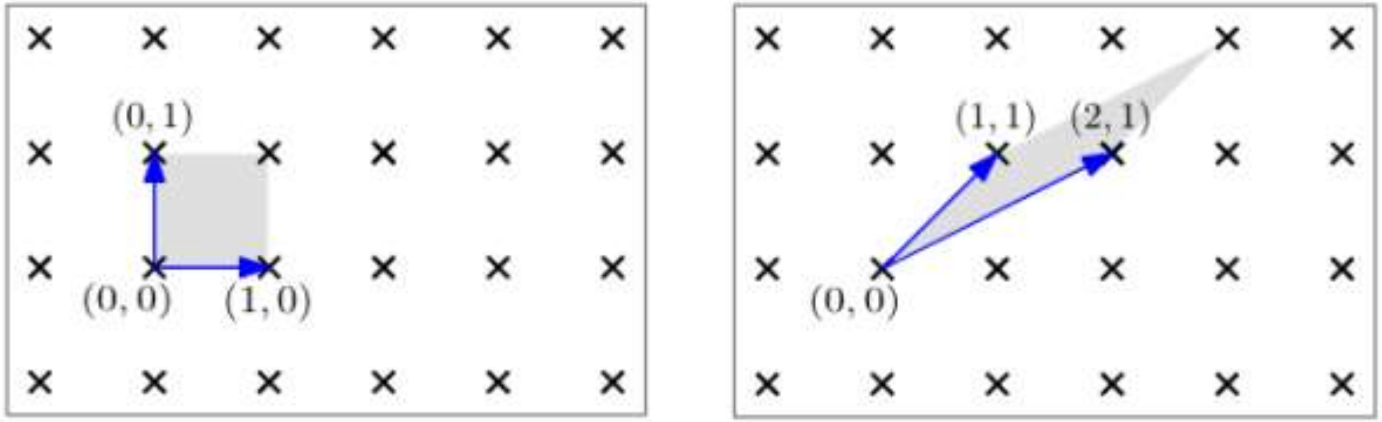


Figure 1: Example of a lattice ($\mathbb{Z}^2$) and 2 possible basis for it [3].

Vandermonde matrix

각 행이 초항이 1인 등비수열로 구성된 행렬

$$V = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \dots & \alpha_m^{n-1} \end{bmatrix}$$

Ring

두 가지 binary operation인 덧셈(+, addition)과 곱셈(· , multiplication)이 정의된 집합 R로 구성되어 있으며, 다음 세 가지 집합의 공리를 만족하는 대수적인 구조

1. 덧셈 공리 (Addition Axioms)
   - $a + b = b + a$ for all a, b in R (that is, $+$ is commutative).
   - $(a + b) + c = a + (b + c)$ for all a, b, c in R (that is, $+$ is associative).
   - There is an element 0 in R such that $a + 0 = a$ for all a in R (that is, 0 is the additive identity).
   - For each a in R there exists $-a$ in R such that $a + (-a) = 0$ (that is, $-a$ is the additive inverse of a).

Ring

2. 곱셈 공리 (Multiplication Axioms)

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in R (that is, $\cdot$ is associative).
- There is an element 1 in R such that $a \cdot 1 = a$ and $1 \cdot a = a$ for all a in R (that is, 1 is the multiplicative identity).

3. 분배 법칙 (Distributive Law)

- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all a, b, c in R (left distributivity).
- $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all a, b, c in R (right distributivity).

Example : 정수 ($\mathbb{Z}$), 유리수($\mathbb{Q}$), 실수 ($\mathbb{R}$), 복소수 ($\mathbb{C}$)

Field

아래와 같은 두 가지 성질을 만족하는 ring

1. Commutative ring : 곱셈이 교환 법칙을 만족하는 ring

   즉, 모든 $a,\ b \in F$에 대하여 $ab = ba$이다.

2. Division ring : 모든 0이 아닌 원소가 invertible한 ring

   즉, 임의의 $a \in F$에 대하여 $a \neq 0$라 하면 $ab = ba = 1$인 $\mathrm{b} \in F$가 존재한다.

Example : ~~정수 ($\mathbb{Z}$)~~, 유리수($\mathbb{Q}$), 실수 ($\mathbb{R}$), 복소수 ($\mathbb{C}$)

Polynomial Ring

Let $[R, +, \cdot]$ be a ring. A polynomial $f(x)$, over R is an expression of the form:

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $n \geq 0$, and $a_0, a_1, a_2, \cdots, a_n \in R$. If $a_n \neq 0$, then the degree of $f(x)$ is n.

The set of all polynomials in the indeterminate x with coefficients in R is denoted by $R[x]$.

Example : $\mathbb{Z}[x]$에는 $1 + x,\ 3 - 2x + 5x^3,\ -4$와 같은 다항식들이 존재한다.

Quotient ring

26.14 Corollary **(Analogue of Corollary 14.5)** Let N be an ideal of a ring R. Then the additive cosets of N form a ring R/N with the binary operations defined by

$$(a+N)+(b+N)=(a+b)+N$$

and

$$(a+N)(b+N)=ab+N.$$

26.15 Definition The ring R/N in the preceding corollary is the **factor ring** (or **quotient ring**) **of** R **by** N. ■

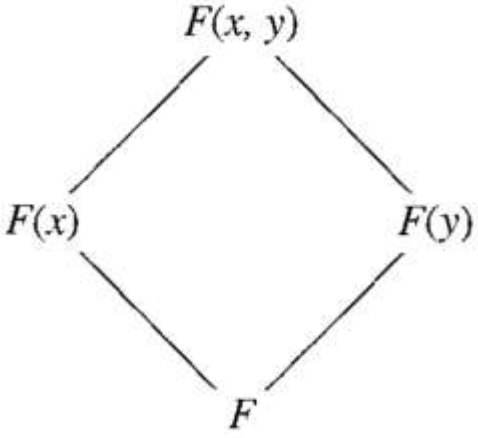
Example : $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$

Extension field

29.1 Definition A field E is an **extension field of a field** F if $F \leq E$.

Example : $\mathbb{C} = \mathbb{R}(i)$

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$



29.3 Theorem (**Kronecker's Theorem**) (**Basic Goal**) Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.

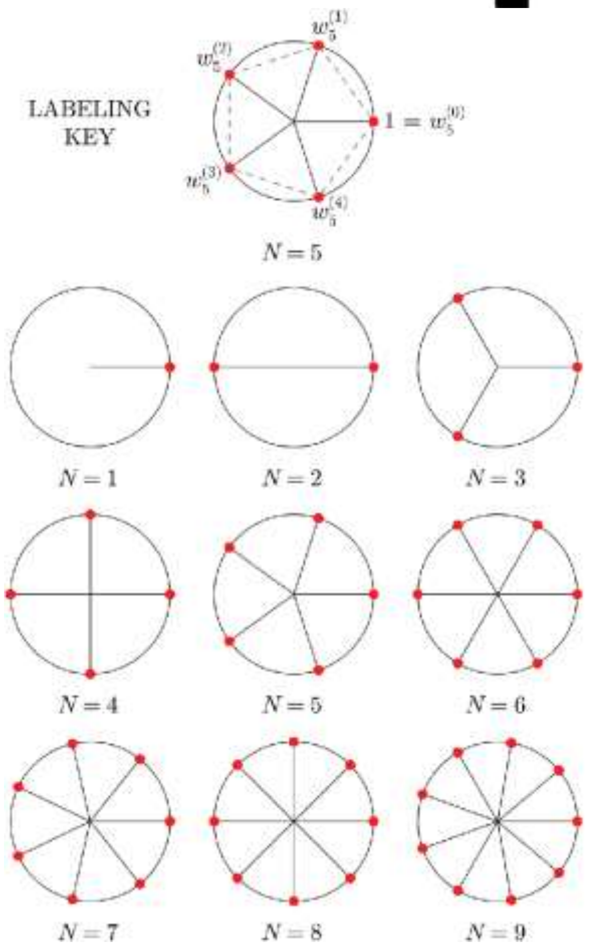
Primitive nth root of unity

33.4 Definition An element α of a field is an ***n*th root of unity** if $\alpha^n = 1$. It is a **primitive *n*th root of unity** if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$. ■

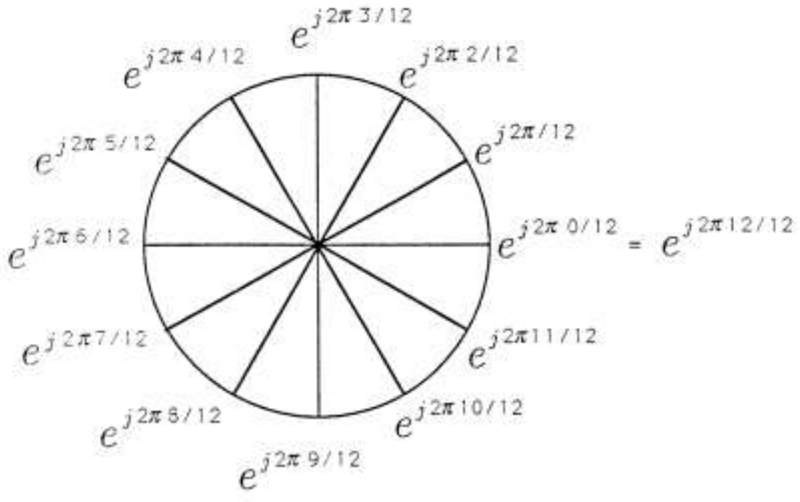
Example : 4th roots of unity : $\pm 1,\ \pm i$

primitive 4th roots of unity : $\pm i$

nth roots of unity : $e^{2\pi i k/n}$ where $1 \leq k \leq n,\ \gcd(k, n) = 1$



Cyclotomic polynomial



55.2 Definition The polynomial

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i)$$

where the α_i are the primitive nth roots of unity in $\overline{F}$, is the ***n*th cyclotomic polynomial over** F. ■

- $\zeta_1 = 1$, so $\Phi_1(x) = x - 1$.
- $\zeta_2 = -1$, so $\Phi_2(x) = x + 1$.
- $\Phi_3(x) = (x - \zeta_3)(x - \zeta_3^2) = x^2 + x + 1$, because $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ and $\zeta_3^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$.
- $\zeta_4 = i$ and the only other primitive 4^{th} root of 1 is $-i$, so $\Phi_4(x) = (x + i)(x - i) = x^2 + 1$.
- An easy shortcut for $\Phi_5(x)$ is this: every 5^{th} root of unity is primitive except for 1, so $\Phi_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$.

중요 : If n is power of 2, $\Phi_n(x) = x^{n/2} + 1$

Cyclotomic ring

$\mathbb{Q}(\zeta_n) \rightarrow$ An extension field that includes all complex roots of the field $\mathbb{Z}[X]/\Phi_n(x)$.

Note that ζ_n is a primitive nth root of unity and $\Phi_n(x)$ is nth cyclotomic polynomial.

If n is power of 2, cyclotomic ring(field) is $\mathbb{Z}[X]/(X^{n/2} + 1)$.

Note that $X^{n/2} + 1$ is nth cyclotomic polynomial, if n is power of 2.

29.3 Theorem (**Kronecker's Theorem**) (**Basic Goal**) Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.

Homomorphism

26.1 Definition A map ϕ of a ring R into a ring R' is a **homomorphism** if

$$\phi(a+b) = \phi(a) + \phi(b)$$

and

$$\phi(ab) = \phi(a)\phi(b)$$

for all elements a and b in R.

Isomorphism

아래와 같은 두 가지 성질을 만족하는 mapping

1. Bijective : 일대일 대응
2. Homomorphism : 연산 보존

* 2개의 ring 사이에 isomorphism이 존재하면 그 두 개의 ring은 isomorphic하다고 이야기한다.

Learning With Errors (LWE)

For a secret $\mathbf{s} \in \mathbb{Z}_q^n$, the LWE distribution $A_{\vec{s},\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is sampled by choosing $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, choosing $e \leftarrow \boxed{\chi}$ and outputting:

error distribution

$$(\mathbf{a}, b = \langle \boldsymbol{s}, \boldsymbol{a} \rangle + e \bmod q)$$

Ring-Learning With Errors (RLWE)

- Matrix multiplication보다 polynomial multiplication이 더 빠르다.
- $\mathbb{Z}_q^n$가 아닌 polynomial ring에서도 LWE가 풀기 어려운 문제이다.

Example :

$$3s_1 + 5s_2 + 8s_3 + e_1 = 27$$

$$9s_1 + 7s_2 + s_3 + e_1 = 31$$

$$s_1 + 2s_2 + s_3 + e_3 = 7$$

$$\begin{bmatrix} 3 & 5 & 7 \\ 9 & 7 & 1 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix} = \begin{bmatrix} 27 \\ 31 \\ 7 \end{bmatrix}$$

$$[A] \cdot [s] + [e] = [b]$$

Parameter

Parameter set

PN13QP218 model :

- 일반적인 “Cyclotomic Ring”에서 정의된 RLWE 문제가 기반이다.
- 실수 기반의 암호화 작업이 아닌 경우에도 잘 동작한다. (ex. Complex number)

```
// PN13QP218 is a default parameter set for
logN=13 and logQP=218
PN13QP218 = ParametersLiteral{
    LogN: 13,
    Q: []uint64{0x1fffec001, // 33 + 5 x 30
        0x3fff4001,
        0x3ffe8001,
        0x40020001,
        0x40038001,
        0x3ffc0001},
    P: []uint64{0x800004001}, // 35
    LogScale: 30,
}
```

Cyclotomic polynomial : $\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(x - \zeta_n{}^k\right)$ when ζ_n is a primitive nth root of unity.

Cyclotomic ring : $\mathbb{Q}(\zeta_n) \rightarrow$ An extension field that includes all complex roots of the field $\mathbb{Z}[X]/(X^n + 1)$.

Note that $X^n + 1$ is $2n$th cyclotomic polynomial, if n is power of 2.

```
// PN13QP202pq is a default (post quantum)
parameter set for logN=13 and logQP=202
PN13QP202pq = ParametersLiteral{
    LogN: 13,
    Q: []uint64{0x1fffec001, // 33 + 5 x 27
        0x8008001,
        0x8020001,
        0x802c001,
        0x7fa8001,
        0x7f74001},
    P: []uint64{0x400018001}, // 34
    LogScale: 27,
}
```

```
CKKS parameters: logN = 13, logSlots = 12, logQP = 218, levels = 6, scale= 1073741824.000000, sigma = 3.200000
```

Parameter set

PN13QP218CI model:

- "Conjugate Invariant Ring"에서 정의된 RLWE 문제가 기반이다.

Cyclotomic Ring : $\mathbb{Q}(\zeta_n) \rightarrow$ An extension field that includes all complex roots of the field $\mathbb{Z}[X]/(X^n + 1)$.

Note that $X^n + 1$ is $2n$th cyclotomic polynomial, if n is power of 2.

Conjugate Invariant Ring : $\mathbb{Q}(\xi_n)$ when $\xi_n \coloneqq \zeta_n + \zeta_n^{-1}$

이 때, $\mathbb{Q}(\xi_n)$가 maximal real subfield가 되기 때문에 아래와 같은 성질이 만족된다.

1. RLWE encryption이 conjugate-invariant ring에서도 동일하게 어려운 문제이다.
2. Ring homomorphism이 정의될 수 있다.
3. 복소수 연산이 불가능한 대신에 앞의 parameter보다 2배 더 많은 plaintext slot을 지원하여, 한 번에 더 많은 데이터를 암호화하고 연산할 수 있다.

```
// PN13QP218CI is a default parameter set for
logN=13 and logQP=218
PN13QP218CI = ParametersLiteral{
    LogN: 13,
    Q: []uint64{0x200038001, // 33 + 5 x 30
        0x3ffe8001,
        0x40020001,
        0x40038001,
        0x3ffc0001,
        0x40080001},
    P:      []uint64{0x800008001}, // 35
    RingType: ring.ConjugateInvariant,
    LogScale: 30,
}
```

```
// PN13QP202CIpq is a default (post quantum)
parameter set for logN=13 and logQP=202
PN13QP202CIpq = ParametersLiteral{
    LogN: 13,
    Q: []uint64{0x1ffffe0001, 0x100050001,
          0xfff88001, 0x100098001,
          0x1000b0001}, // 37 + 4 x 32
    P: []uint64{0x1ffffc0001},   // 37
    RingType: ring.ConjugateInvariant,
    LogScale: 32,
}
```

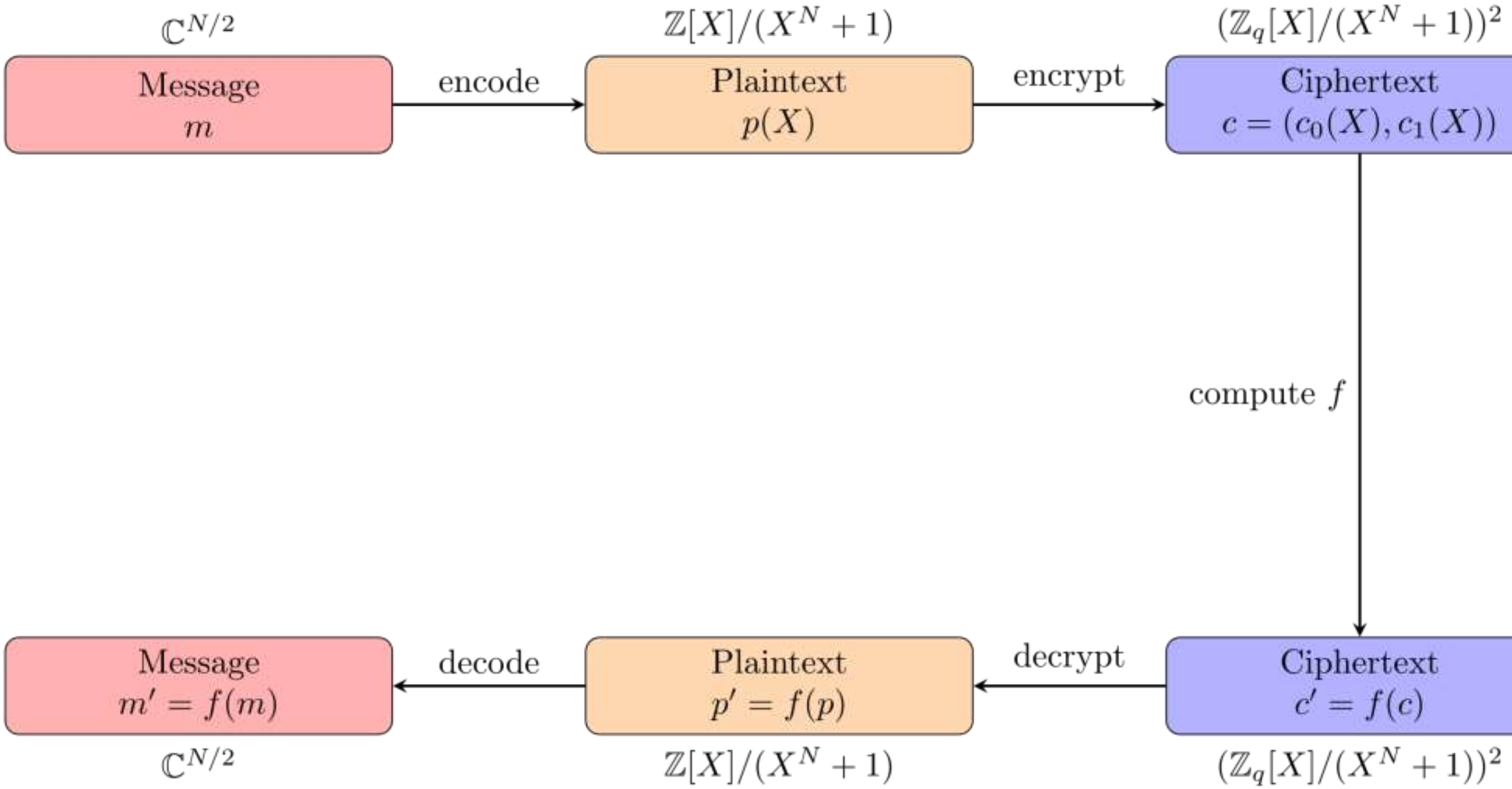
```
CKKS parameters: logN = 13, logSlots = 13, logQP = 219, levels = 6, scale= 1073741824.000000, sigma = 3.200000
```

```
(3.44+57.25i)  (59.29+24.11i)  (64.04+63.39i)  (95.69+6.60i)  (97.38+3.69i)  (50.38+7.09i)  (34.70+72.99i)  (40.69+23.00i)  (13.91+32.70i)  (59.94+30.31i)  (99.16+89.08i)
(3.44-0.00i)   (59.29+0.00i)   (64.04-0.00i)   (95.69-0.00i)  (97.38+0.00i)  (50.38-0.00i)  (34.70+0.00i)   (40.69+0.00i)   (13.91-0.00i)   (59.94+0.00i)   (99.16-0.00i)
```

Kim, Duhyeong, and Yongsoo Song. "Approximate homomorphic encryption over the conjugate-invariant ring." *Information Security and Cryptology–ICISC 2018: 21st International Conference, Seoul, South Korea, November 28–30, 2018, Revised Selected Papers 21*. Springer International Publishing, 2019. (https://eprint.iacr.org/2018/952.pdf)

Encoding / Decoding

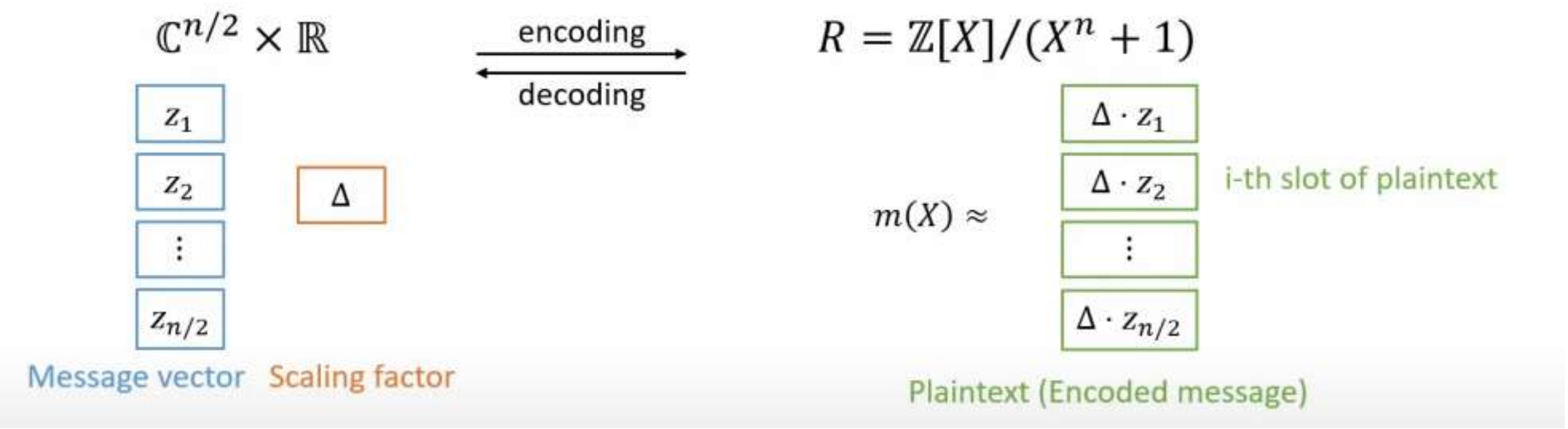
CKKS scheme



$\mathbb{C}^{N/2}$
Message
m
encode
$\mathbb{Z}[X]/(X^N+1)$
Plaintext
$p(X)$
encrypt
$(\mathbb{Z}_q[X]/(X^N+1))^2$
Ciphertext
$c = (c_0(X), c_1(X))$
compute f
Ciphertext
$c' = f(c)$
$(\mathbb{Z}_q[X]/(X^N+1))^2$
decrypt
Plaintext
$p' = f(p)$
$\mathbb{Z}[X]/(X^N+1)$
decode
Message
$m' = f(m)$
$\mathbb{C}^{N/2}$

Encode & Decode

- $\mathsf{Ecd}(\boldsymbol{z};\Delta)$. For a $(N/2)$-dimensional vector $\boldsymbol{z}=(z_j)_{j\in T}\in\mathbb{Z}[i]^{N/2}$ of Gaussian integers, compute the vector $\left\lfloor \Delta\cdot\pi^{-1}(\boldsymbol{z})\right\rceil_{\sigma(\mathcal{R})}$. Return its inverse with respect to canonical embedding map.
- $\mathsf{Dcd}(m;\Delta)$. For an input polynomial $m(X)\in\mathcal{R}$, compute the corresponding vector $\pi\circ\sigma(m)$. Return the closest vector of Gaussian integers $\boldsymbol{z}=(z_j)_{j\in T}\in\mathbb{Z}[i]^{N/2}$ after scaling, i.e., $z_j=\left\lfloor \Delta^{-1}\cdot m(\zeta_M^j)\right\rceil$ for $j\in T$.



Encode & Decode

$$\mathbb{C}^{\phi(M)/2} \xrightarrow{\pi^{-1}} \mathbb{H} \xrightarrow{\lfloor\cdot\rceil_{\sigma(R)}} \sigma(R) \xrightarrow{\sigma^{-1}} R$$

$$\boldsymbol{z}=(z_i)_{i\in T} \longmapsto \pi^{-1}(\boldsymbol{z}) \longmapsto \lfloor \Delta\pi^{-1}(\boldsymbol{z})\rceil_{\sigma(R)} \longmapsto \sigma^{-1}\left(\lfloor \Delta\pi^{-1}(\boldsymbol{z})\rceil_{\sigma(R)}\right)$$

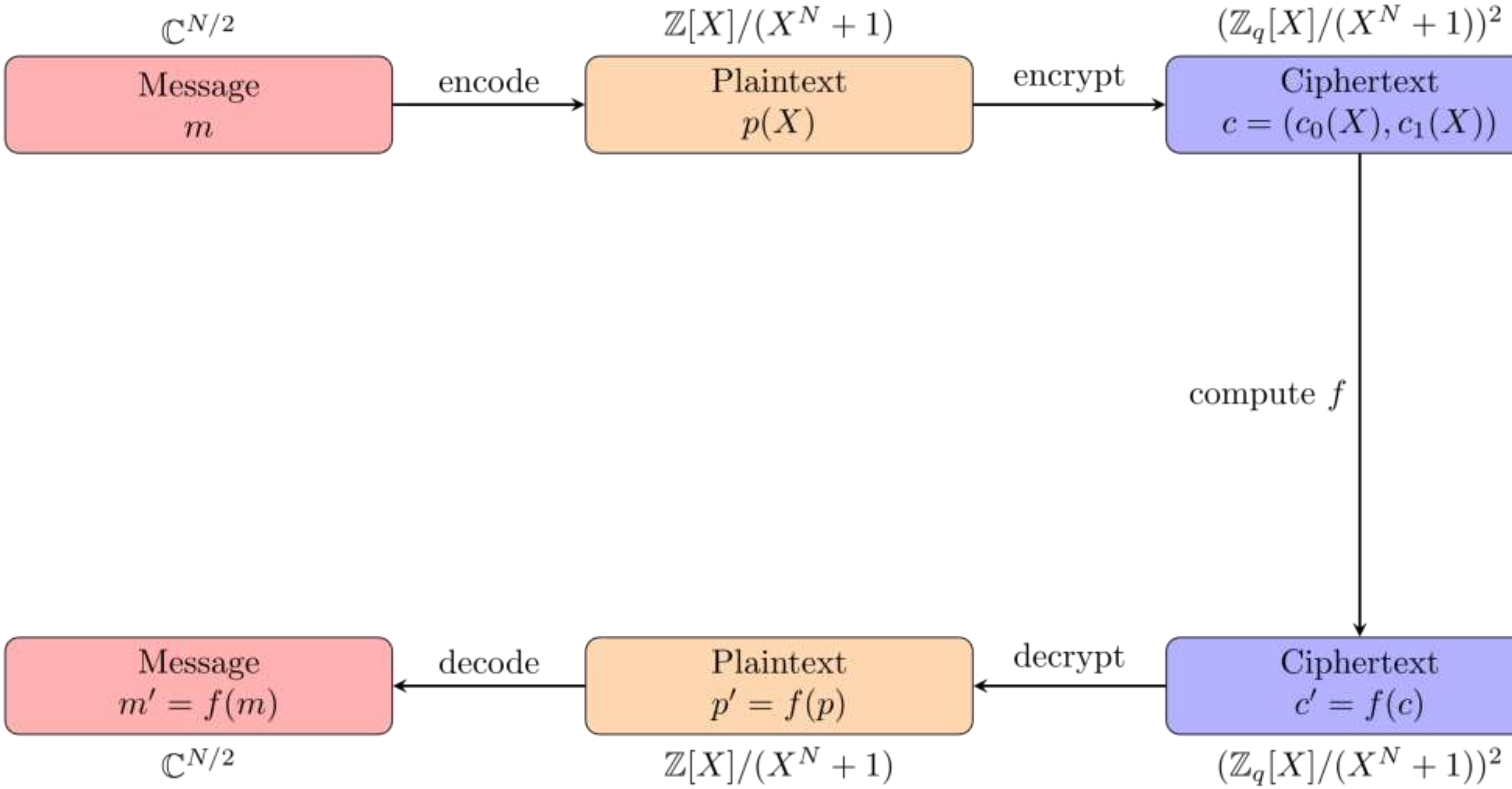
$$\mathbb{H} = \{(z_j)_{j\in\mathbb{Z}_M^*} : z_{-j} = \overline{z_j}, \forall j \in \mathbb{Z}_M^*\} \subseteq \mathbb{C}^{\Phi(M)}$$

1. $\mathbb{C}^{N/2}$의 원소 $\boldsymbol{z}$를 취합니다.
2. $\pi^{-1}(z)$를 사용하여 확장합니다.
3. 정밀도를 위해 Δ로 곱합니다.
4. $\sigma(R)$에 투영합니다: $\lfloor\Delta\pi^{-1}(z)\rceil_{\sigma(R)} \in \sigma(R)$
5. σ를 사용하여 인코딩합니다: $m(X) = \sigma^{-1}\left(\lfloor\Delta\pi^{-1}(\boldsymbol{z})\rceil_{\{\sigma(R)\}}\right) \in R$.

코드 참고!

Encrypt / Decrypt

CKKS scheme



$\mathbb{C}^{N/2}$
Message
m
encode
$\mathbb{Z}[X]/(X^N+1)$
Plaintext
$p(X)$
encrypt
$(\mathbb{Z}_q[X]/(X^N+1))^2$
Ciphertext
$c = (c_0(X), c_1(X))$
compute f
Ciphertext
$c' = f(c)$
$(\mathbb{Z}_q[X]/(X^N+1))^2$
decrypt
Plaintext
$p' = f(p)$
$\mathbb{Z}[X]/(X^N+1)$
decode
Message
$m' = f(m)$
$\mathbb{C}^{N/2}$

- $\mathcal{ZO}(0.5)$: 0과 1사이의 값을 갖는 균일 분포
- $\mathcal{DG}(\sigma^2)$: 이산 가우시안 분포 / σ^2는 분포의 분산

GenKey & Enc, Dec

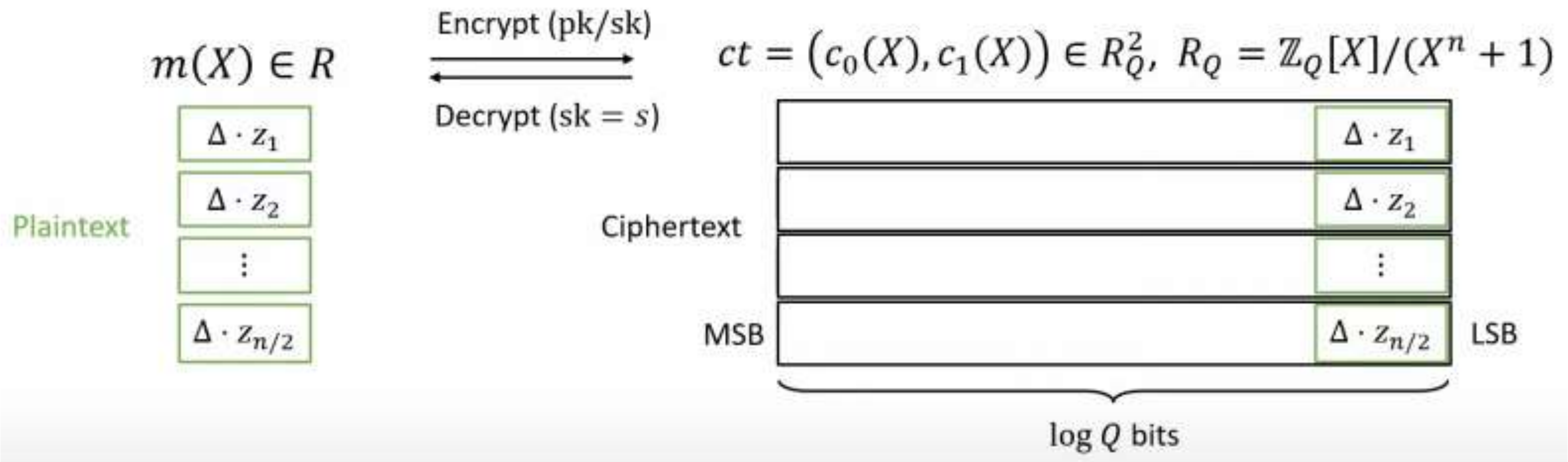
- Secret Key Generation

$$\boldsymbol{s} \leftarrow (1, \mathrm{s}'[1], \ldots, \mathrm{s}'[\mathrm{n}]) \in \mathrm{R}_{\mathrm{q}}^{\mathrm{n}+1}, \text{where } \mathrm{s}' \leftarrow \chi^{\mathrm{n}}$$

- Public Key Generation

$$\mathrm{pk} = \mathrm{A}, \text{where } \mathrm{A} \cdot \boldsymbol{s} = 2\mathrm{e} \text{ for } \mathrm{e} \leftarrow \chi^{\mathrm{n}}$$

- $\mathsf{Enc}_{pk}(m)$. Sample $v \leftarrow \mathcal{ZO}(0.5)$ and $e_0, e_1 \leftarrow \mathcal{DG}(\sigma^2)$. Output $v \cdot pk + (m + e_0, e_1) \pmod{q_L}$.
- $\mathsf{Dec}_{sk}(\boldsymbol{c})$. For $\boldsymbol{c} = (b, a)$, output $b + a \cdot s \pmod{q_\ell}$.



CNN 사용예시

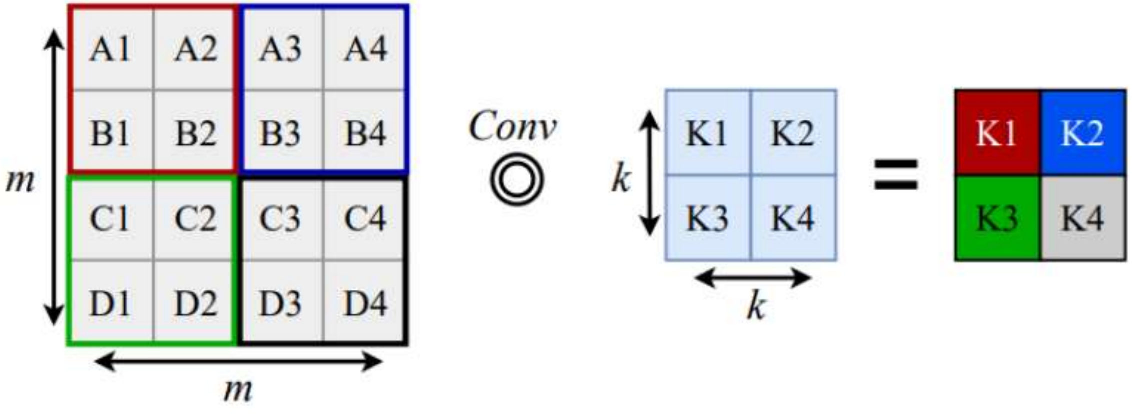
https://github.com/hm-choi/uni-henn/tree/develop

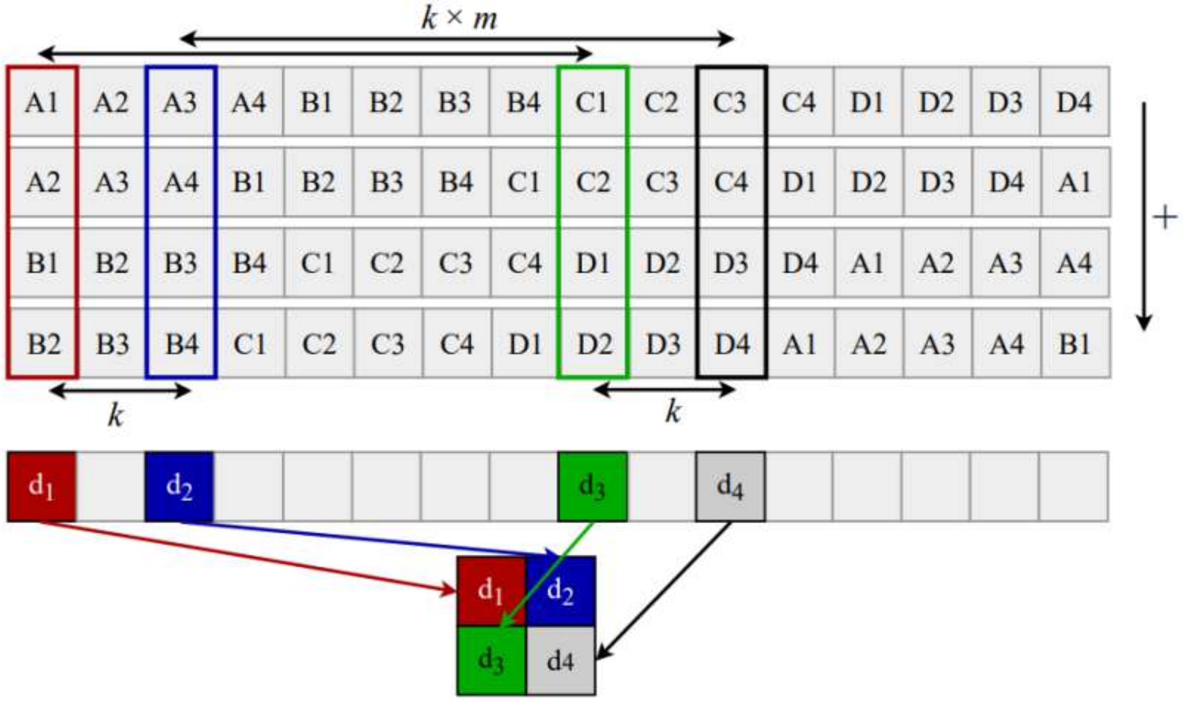
UniHENN: Designing Faster and More Versatile Homomorphic Encryption-based CNNs without `im2col`

https://github.com/hm-choi/uni-henn/tree/develop

HYUNMIN CHOI[1 2], JIHUN KIM[1], SEUNGHO KIM[1], SEONHYE PARK[1], JEONGYONG PARK[1], WONBIN CHOI[2], HYOUNGSHICK KIM[1]
[1]Sungkyunkwan University, Republic of Korea
[2]NAVER Cloud, Republic of Korea
Corresponding author: Hyoungshick Kim (hyoung@skku.edu).

II. Construction of the Convolutional Layer





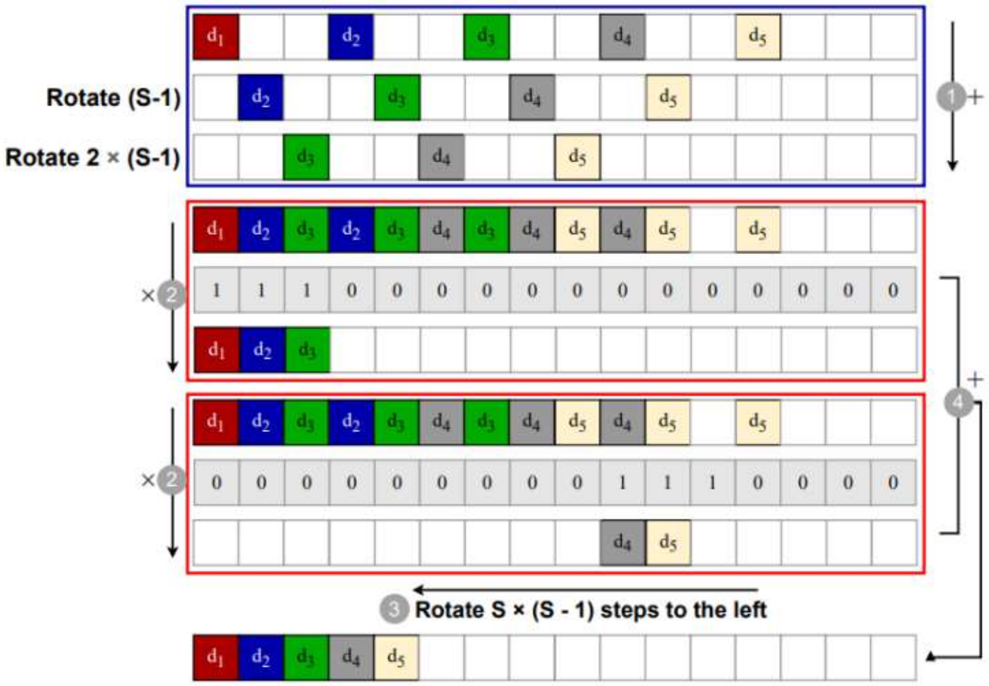
UniHENN: Designing Faster and More Versatile Homomorphic Encryption-based CNNs without im2col

https://github.com/hm-choi/uni-henn/tree/develop

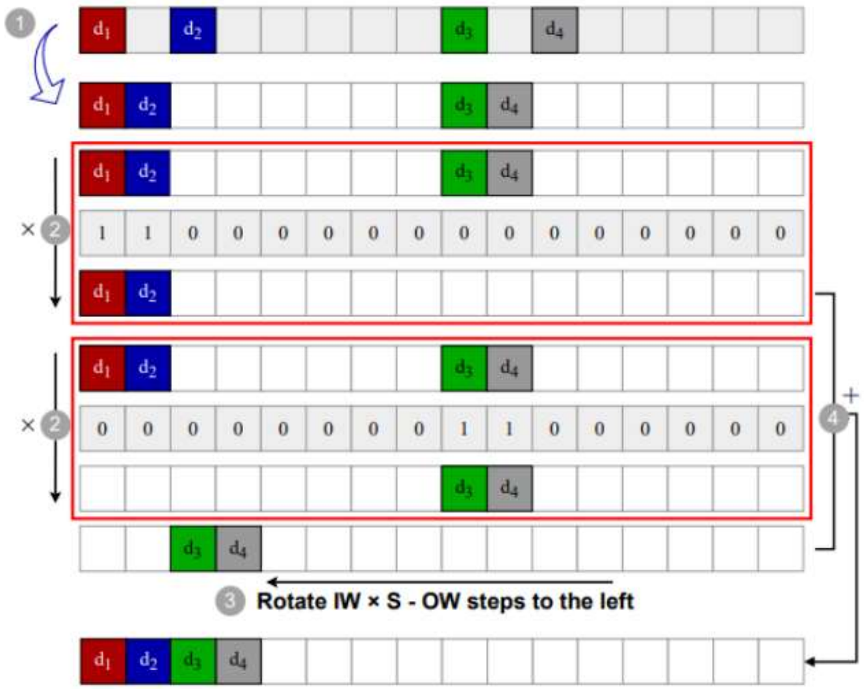
HYUNMIN CHOI[1 2], JIHUN KIM[1], SEUNGHO KIM[1], SEONHYE PARK[1], JEONGYONG PARK[1], WONBIN CHOI[2], HYOUNGSHICK KIM[1]
[1]Sungkyunkwan University, Republic of Korea
[2]NAVER Cloud, Republic of Korea
Corresponding author: Hyoungshick Kim (hyoung@skku.edu).

IV. Construction of the Flatten Layer

① Removing the row interval



② Removing the column interval



UniHENN: Designing Faster and More Versatile Homomorphic Encryption-based CNNs without `im2col`

https://github.com/hm-choi/uni-henn/tree/develop

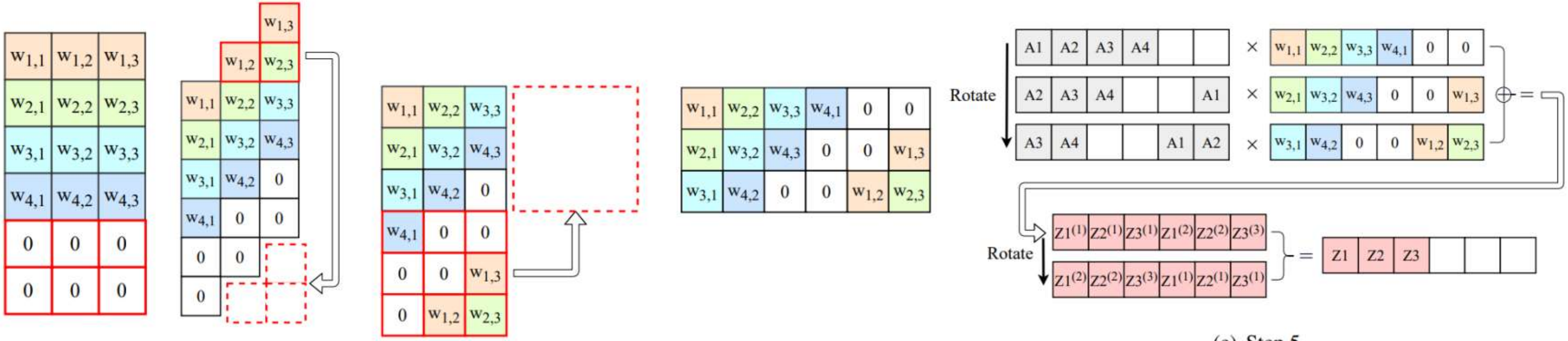
HYUNMIN CHOI[1 2], JIHUN KIM[1], SEUNGHO KIM[1], SEONHYE PARK[1], JEONGYONG PARK[1], WONBIN CHOI[2], HYOUNGSHICK KIM[1]

[1]Sungkyunkwan University, Republic of Korea

[2]NAVER Cloud, Republic of Korea

Corresponding author: Hyoungshick Kim (hyoung@skku.edu).

V. Construction of the Fully Connected (FC) Layer



(a) Step 1 (b) Step 2 (c) Step 3 (d) Step 4 (e) Step 5