

<Slot To Coeff>

#1

$$\left[ \frac{pt^{1st}}{\Delta}, \frac{pt^{2nd}}{\Delta} \right] \xrightarrow{\text{bit Reversed}} \Delta$$

$$\xrightarrow{ct_{EvalMod}}$$

$$\in (R_{Q_{L-10}}^2)^2$$

multiplication  
by  $U_0 = [A[0] \times A[1] \times A[2]]$

$$\left[ \frac{U_0 pt^{1st}}{\Delta}, \frac{U_0 pt^{2nd}}{\Delta} \right] \xrightarrow{\Delta^4}$$

$$\xrightarrow{[CT_1]}$$

$$\in (R_{Q_{L-10}}^2)^2$$

Choose primes  $q[L-11] \simeq \Delta$

$q[L-12] \simeq \Delta$

$q[L-13] \simeq \Delta$

RS

$$[ct_2, ct_3] \in (R_{Q_{L-13}}^2)^2$$

$$\left[ \frac{U_0 pt^{1st}}{\Delta}, \frac{U_0 pt^{2nd}}{\Delta} \right] \xrightarrow{\Delta}$$

$$\Sigma \in \mathbb{C}^{\frac{N}{2}}$$

$$ct_2 + (pt_i) * ct_3 \in R_{Q_{L-13}}^2$$

$$\parallel$$
  
$$ct_{stc}$$

$$\parallel$$
  
$$U_0 \frac{pt^{1st}}{\Delta} + i U_0 \frac{pt^{2nd}}{\Delta}$$

```
template <int L, int DNUM, int K>
```

```
void SlotToCoeff_logN_10 (const uint64_t q[L],
                           const uint64_t P[K], uint64_t Delta,
                           const SparseComplexMatrix <1<<9, 2η> A[3],
                           const uint64_t rkey[3][2η][DNUM][2][DNUM*K+K][1<<10],
                           const uint64_t c^EvalMod [2][2][L][1<<10],
                           uint64_t c^stc [2][L-3][1<<10]) {
```

```
const N = 1<<10;
```

```
uint64_t c^1 [2][2][L][N];
```

```
for (int i=0; i<2; i++)
```

```
for (int j=0; j<2; j++)
```

```
for (int k=0; k<L; k++)
```

```
for (int w=0; w<N; w++)
```

```
c^1[i][j][k][w] = c^EvalMod [i][j][k][w];
```

```
for (int n=2; n>=0; n--) {
```

```
uint64_t temp [2][2][L][N];
```

```
for (int i=0; i<2; i++)
```

```
linearTransformation <N, 10, L, DNUM, K, 2η> (A[n], Delta, q, P, rkey[n],
```

```
c^1[i], temp[i]);
```

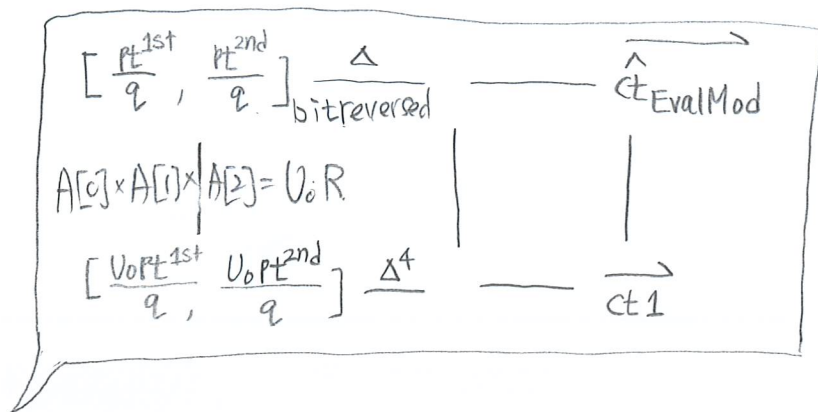
```
for (int i=0; i<2; i++)
```

```
for (int j=0; j<2; j++)
```

```
for (int k=0; k<L; k++)
```

```
for (int w=0; w<N; w++)
```

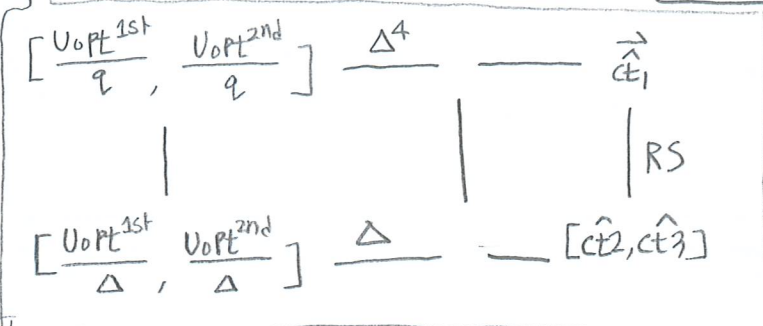
```
c^1[i][j][k][w] = temp[i][j][k][w]
```



```
}
```

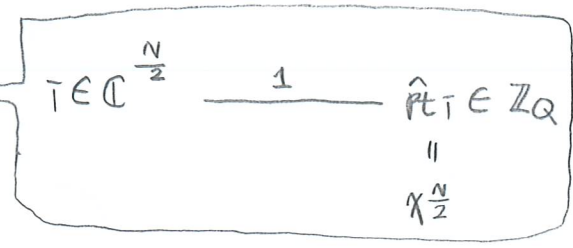
```

uint64_t c2[2][L+3][N];
uint64_t c3[2][L+3][N];
RS_hat <N, L, L+3>(q, c1[0], c2);
RS_hat <N, L, L+3>(q, c1[1], c3);
    
```



```

uint64_t pT[L+3][N];
for (int i=0; i<L+3; i++) {
    for (int j=0; j<N; j++) pT[i][j] = 0;
    pT[i][N/2] = 1;
}
ntt<N, L+3>(q, pT);
    
```



```

for (int i=0; i<2; i++)
for (int j=0; j<L+3; j++)
for (int k=0; k<N; k++) {
    cT_sec[i][j][k] = (c2[i][j][k] + mul_mod(pT[i][j][k], c3[i][j][k], q[j])) % q[j];
}
    
```

$$\hat{c}_{Tsec} = \hat{c}_2 + (\hat{p}_T) * \hat{c}_3$$

$$\begin{array}{ccccc} z \in \mathbb{C}^{\frac{N}{2}} & \xrightarrow{\Delta} & pt & \xrightarrow{\quad} & ct \in R_q^2 \\ | & & | & & | \text{ mod } U_p \\ & \xrightarrow{\Delta} & pt + qI & \xrightarrow{\quad} & ct \in R_{Q_L}^2 \end{array}$$

$$\begin{array}{ccc} \xrightarrow{\quad} & & \left\{ \begin{array}{l} \text{CoeffToSlot} \\ [q[L-1] \leq 2^{50} \\ [q[L-2] \leq 12 \cdot 2^{50} \\ [q[L-3] \leq 2^{50} \end{array} \right\} \\ \frac{1}{12} \left( \frac{pt}{q} + I \right) & \xrightarrow{q} & \vec{ct}_{cts} \in (R_{Q_{L-3}}^2)^2 \end{array}$$

$$\begin{array}{ccc} & & \left\{ \begin{array}{l} \text{EvalMod} \\ [q[L-4], \dots, q[L-10] \leq 2^{60}] \end{array} \right\} \\ \frac{pt}{q} & \xrightarrow{q} & \vec{ct}_{evalmod} \in (R_{Q_{L-10}}^2)^2 \end{array}$$

$$\begin{array}{ccc} & & | \\ \frac{pt}{\Delta} & \xrightarrow{\Delta} & \vec{ct}_{evalmod} \in (R_{Q_{L-10}}^2)^2 \end{array}$$

$$\begin{array}{ccc} & & \left\{ \begin{array}{l} \text{SlotToCoeff} \\ [q[L-11], \dots, q[L-13] \leq 2^{50}] \end{array} \right\} \\ z \in \mathbb{C}^{\frac{N}{2}} & \xrightarrow{\Delta} & \frac{pt}{\Delta} \xrightarrow{\quad} ct_{stc} \in R_{Q_{L-13}}^2 \end{array}$$