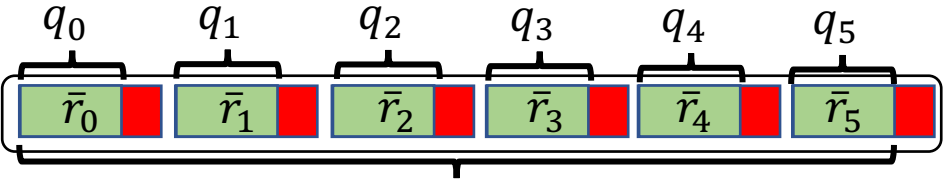


Level

Modulus

Scale

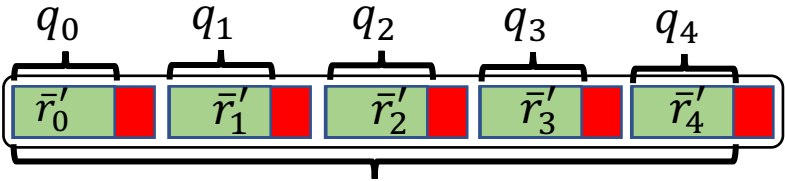
6



$$S_6$$

$$Q_6 = q_0 q_1 q_2 q_3 q_4 q_5$$

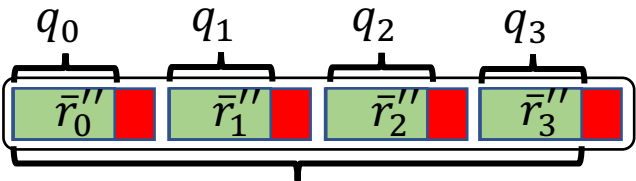
5



$$S_5 = S_6^2 / q_5$$

$$Q_5 = q_0 q_1 q_2 q_3 q_4 = Q_6 / q_5$$

4



$$S_4 = S_5^2 / q_4$$

$$Q_4 = q_0 q_1 q_2 q_3 = Q_5 / q_4$$

⋮

⋮

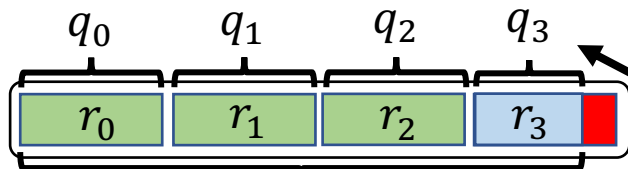
⋮

Level

Modulus

Scale

6

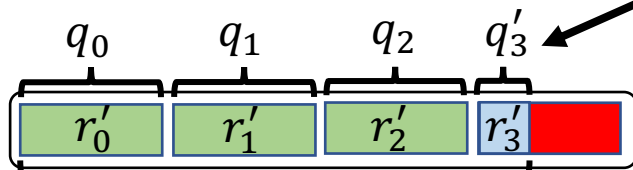


$$Q_6 = q_0 q_1 q_2 q_3$$

$S_6$

$\neq$

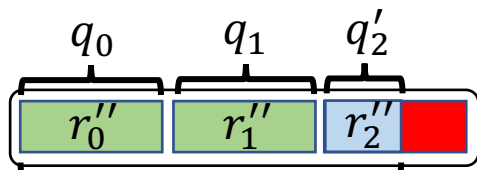
5



$$Q_5 = q_0 q_1 q_2 q'_3 = Q_6 q'_3 / q_3$$

$$S_5 = S_6^2 q'_3 / q_3$$

4



$$Q_4 = q_0 q_1 q'_2 = Q_5 q'_2 / q_2 q'_3$$

$$S_4 = S_5^2 q'_2 / q_2 q'_3$$

$\vdots$

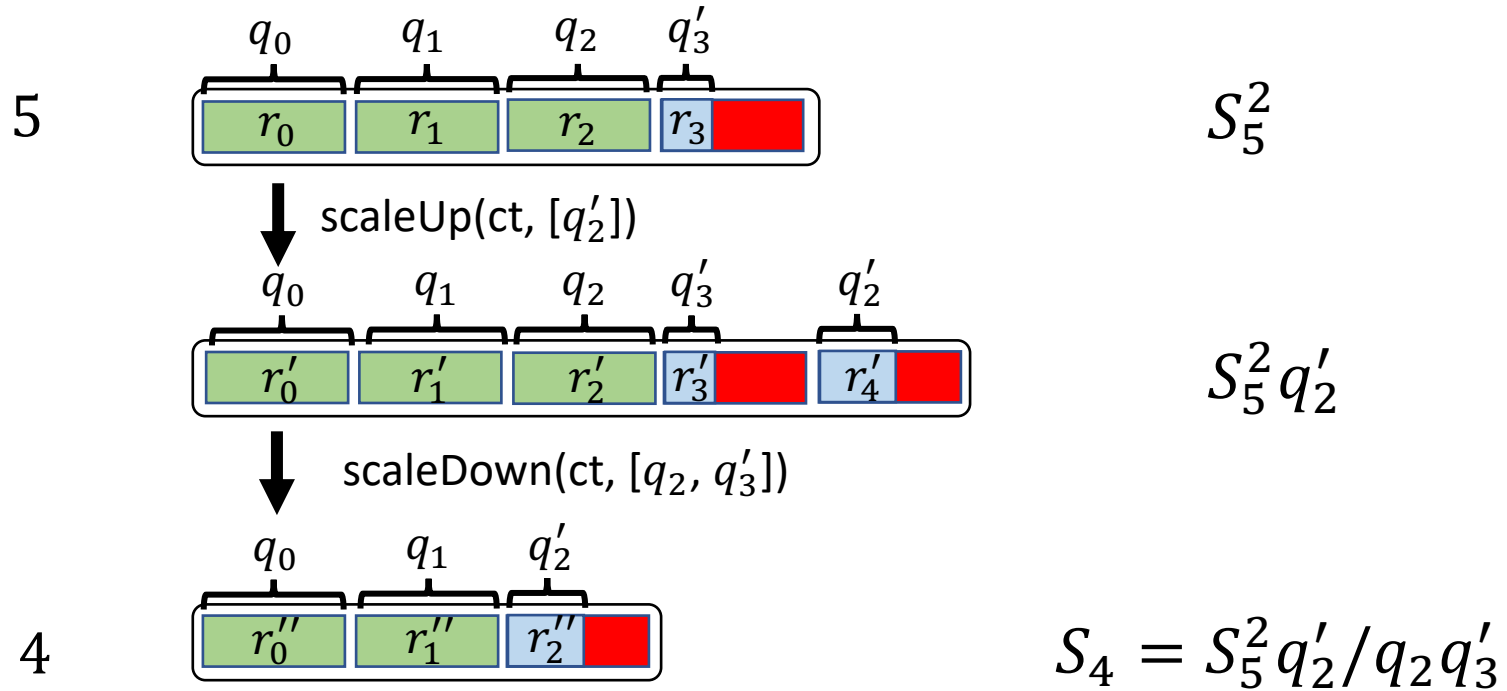
$\vdots$

$\vdots$

Level

Modulus

Scale

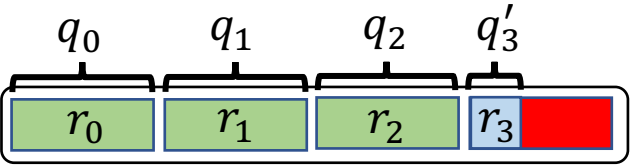


Level

Modulus

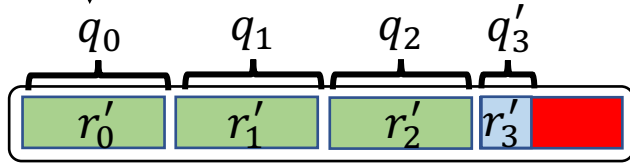
Scale

5



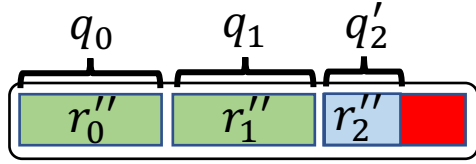
$S_5$

↓  $\text{mulConst}(\text{ct}, K=S_4q'_3/S_5q'_2)$



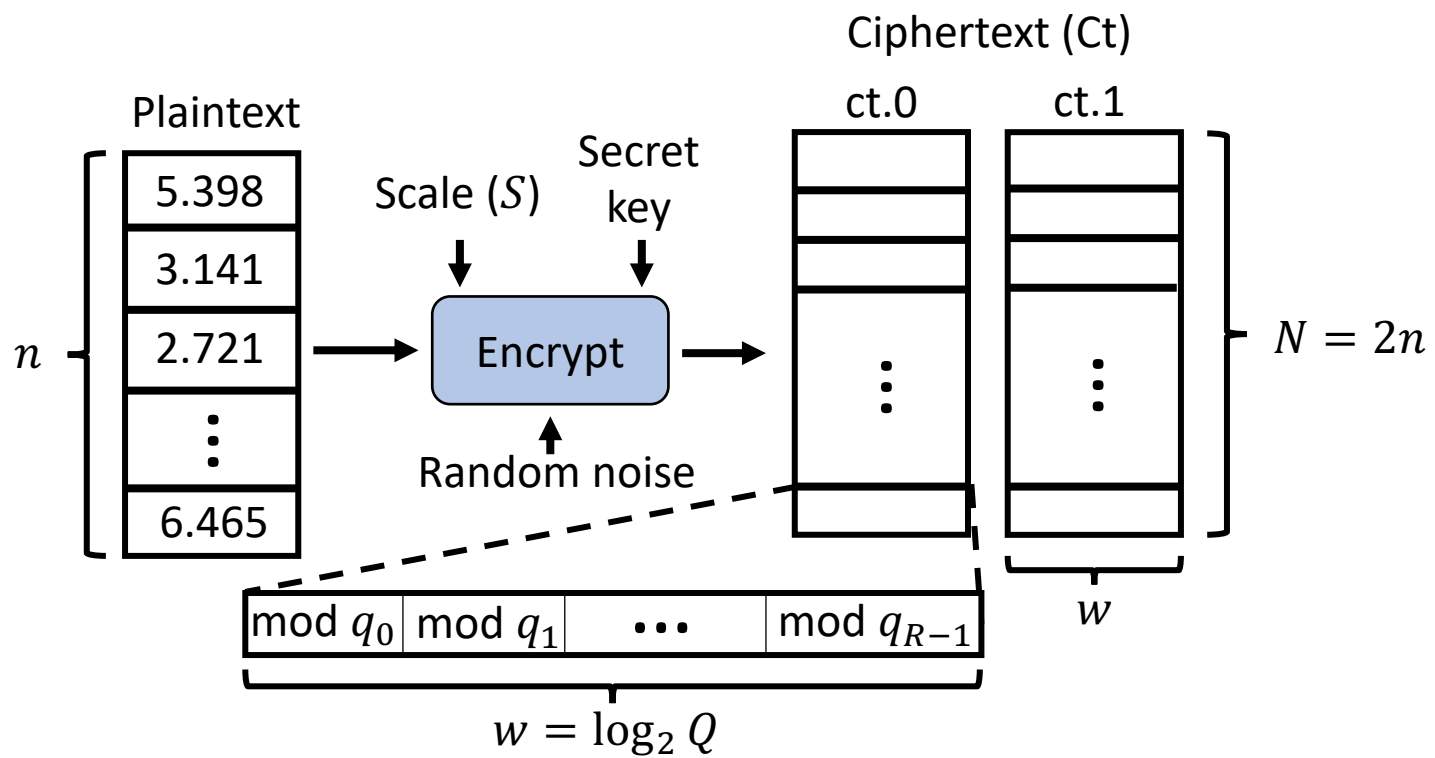
$S_4q'_3/q'_2$

↓  $\text{bpRescale}(\text{ct})$

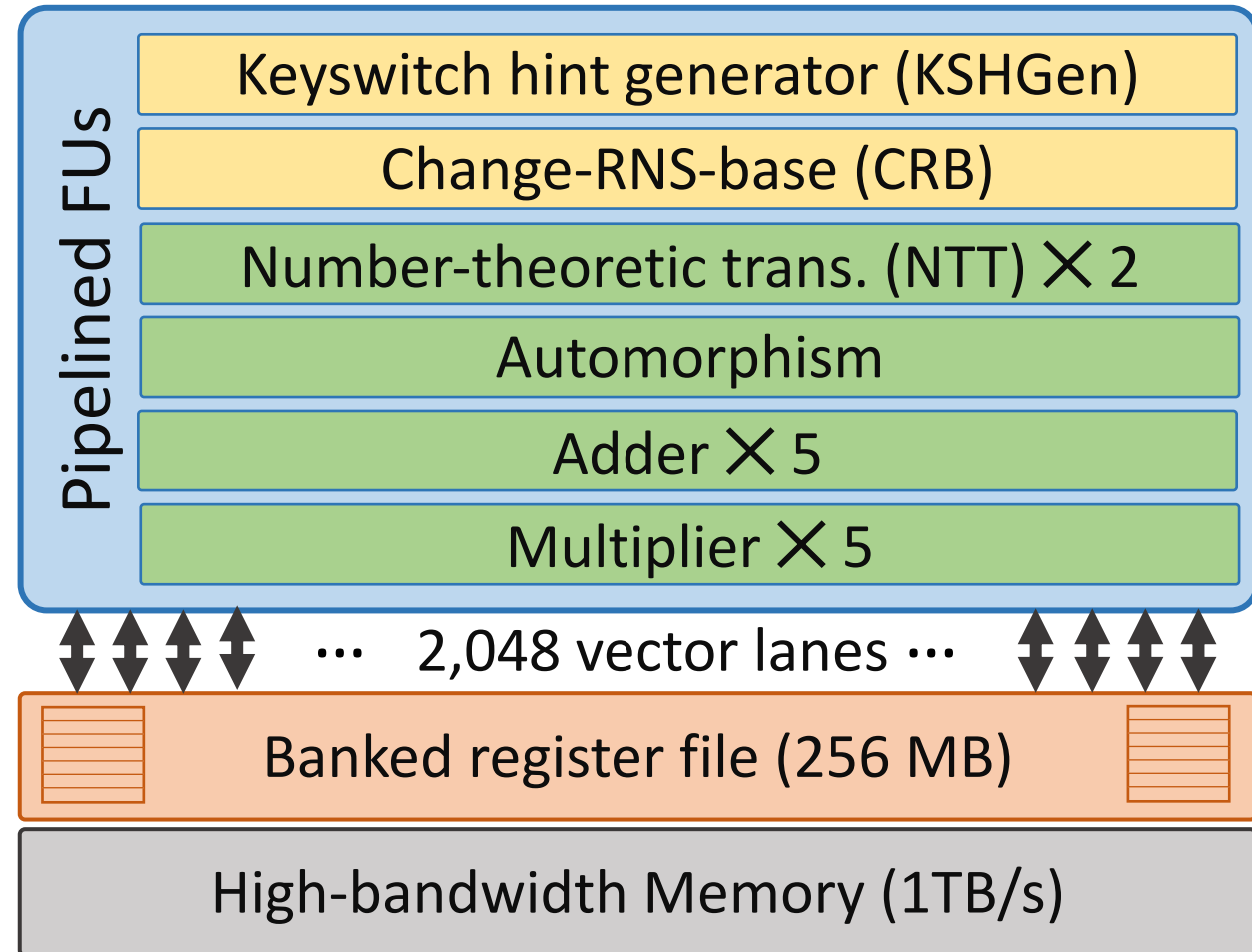


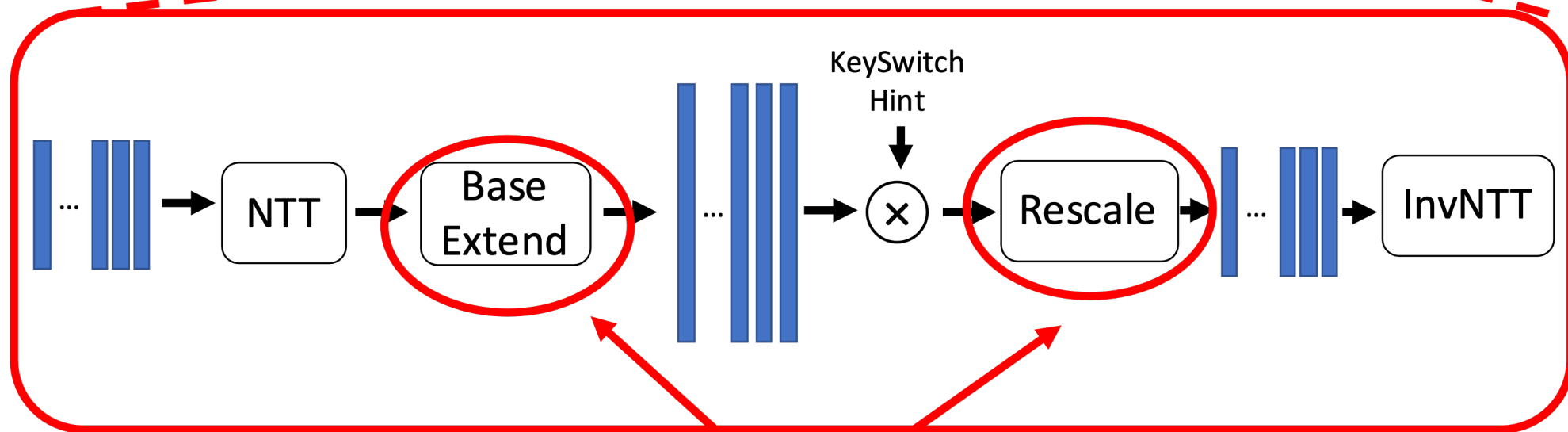
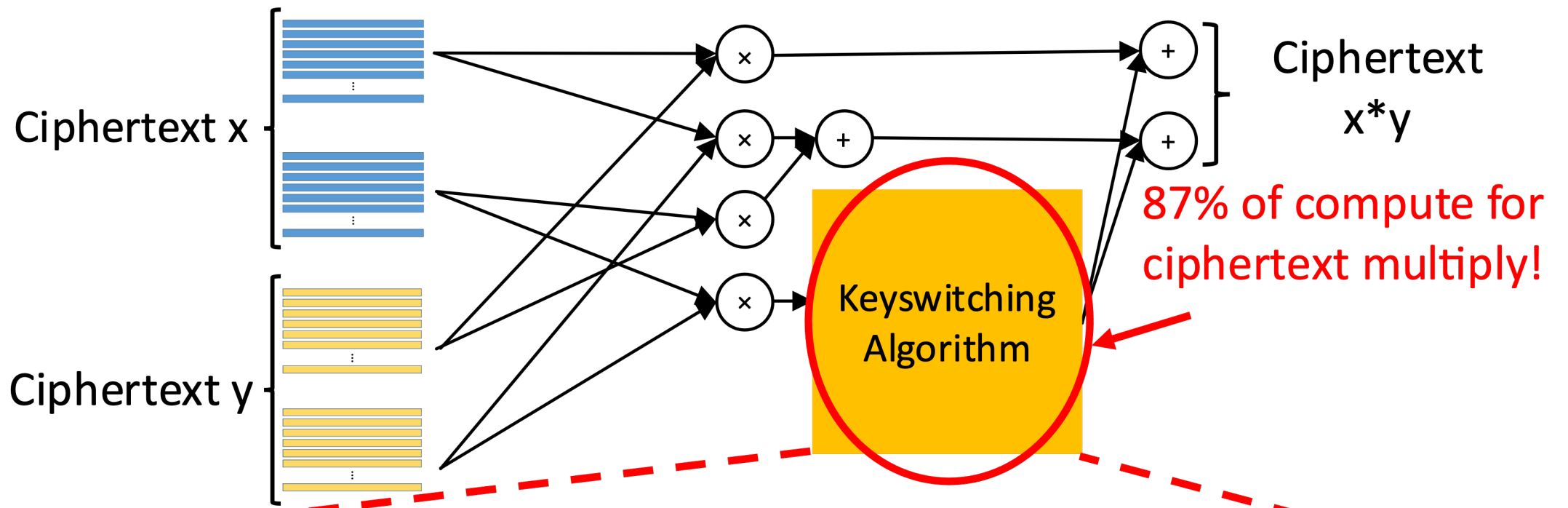
4

$S_4$



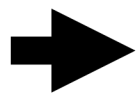








Client



Encrypt



1

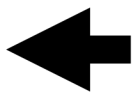


5

Decrypt



"Cat"



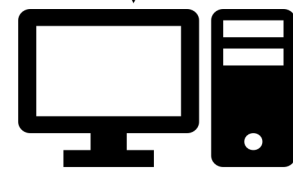
Trust barrier



2

3

4



FHE Server

XwrfvAuw3

# Old Polynomial Layout

Polynomial (vector of RnsInt's)

Coefficient (vector of residues)

64-bit residue



⋮



# New Polynomial Layout

Polynomial (vector of residue polynomials)

