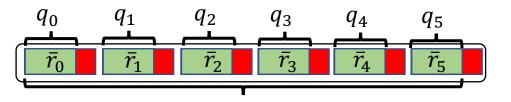
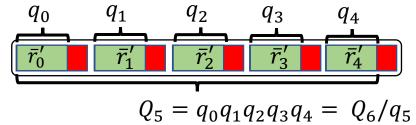


 S_6

6

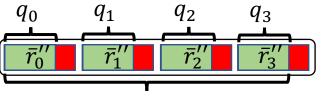


$$Q_6 = q_0 q_1 q_2 q_3 q_4 q_5$$



$$S_5 = S_6^2/q_5$$

4

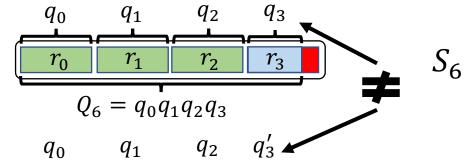


$$S_4 = S_5^2 / q_4$$

:

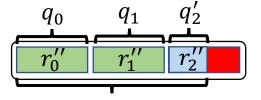
 $Q_4 = q_0 q_1 q_2 q_3 = Q_5/q_4$

•



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

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



$$S_4 = S_5^2 q_2' / q_2 q_3'$$

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



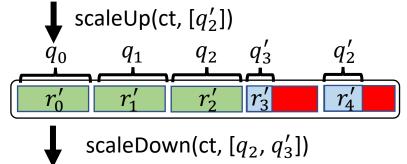
Modulus

Scale

$$q_0 \qquad q_1 \qquad q_2 \qquad q_3'$$

$$r_0 \qquad r_1 \qquad r_2 \qquad r_3$$

$$S_{5}^{2}$$

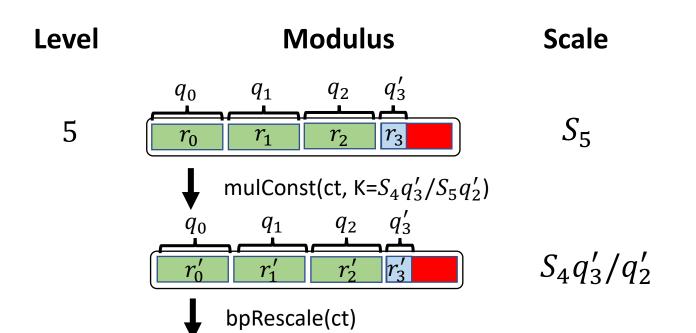


$$S_5^2 q_2'$$

$$q_{0} \quad q_{1} \quad q'_{2}$$

$$q'_{0} \quad r''_{1} \quad r''_{2} \quad q'_{2}$$

$$S_4 = S_5^2 q_2' / q_2 q_3'$$

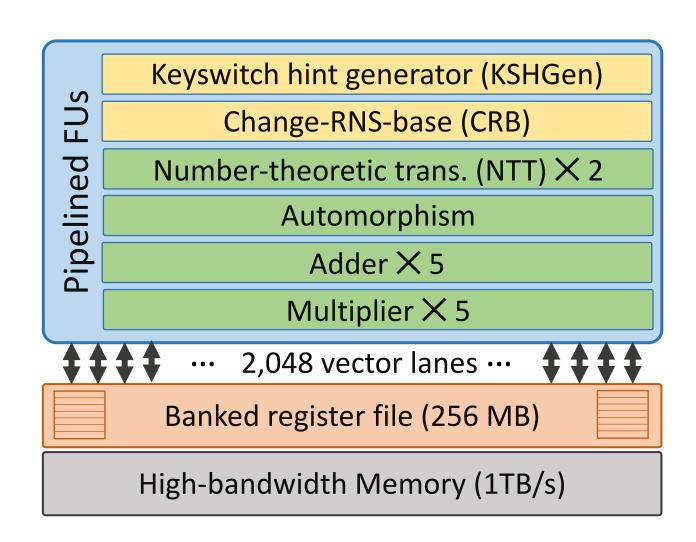


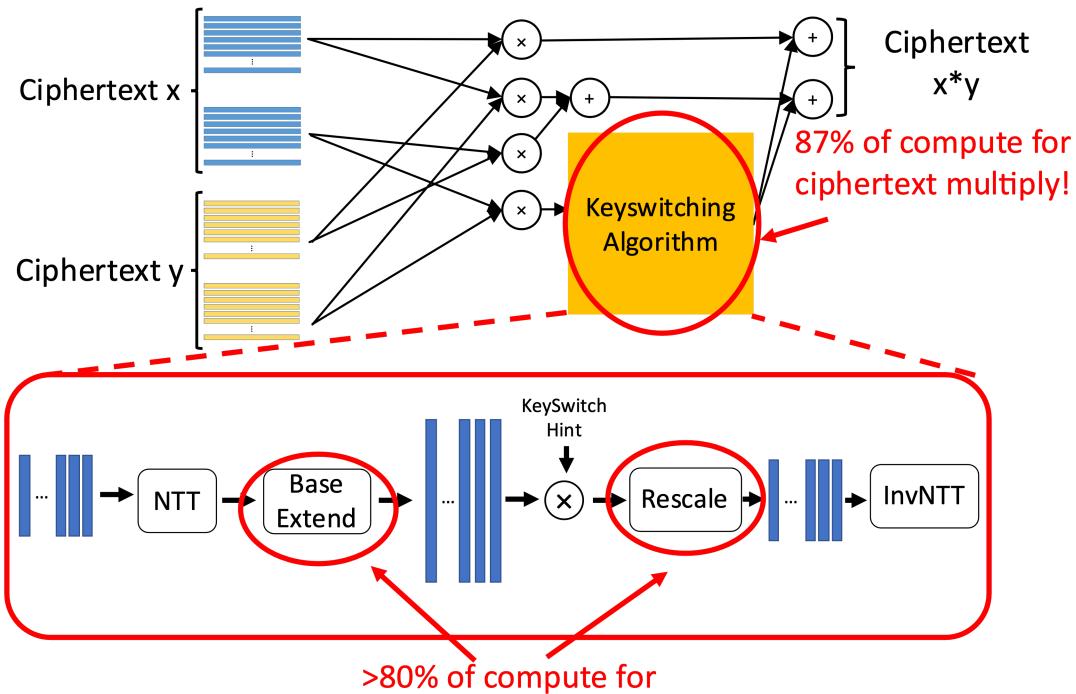
 S_4

 q_1

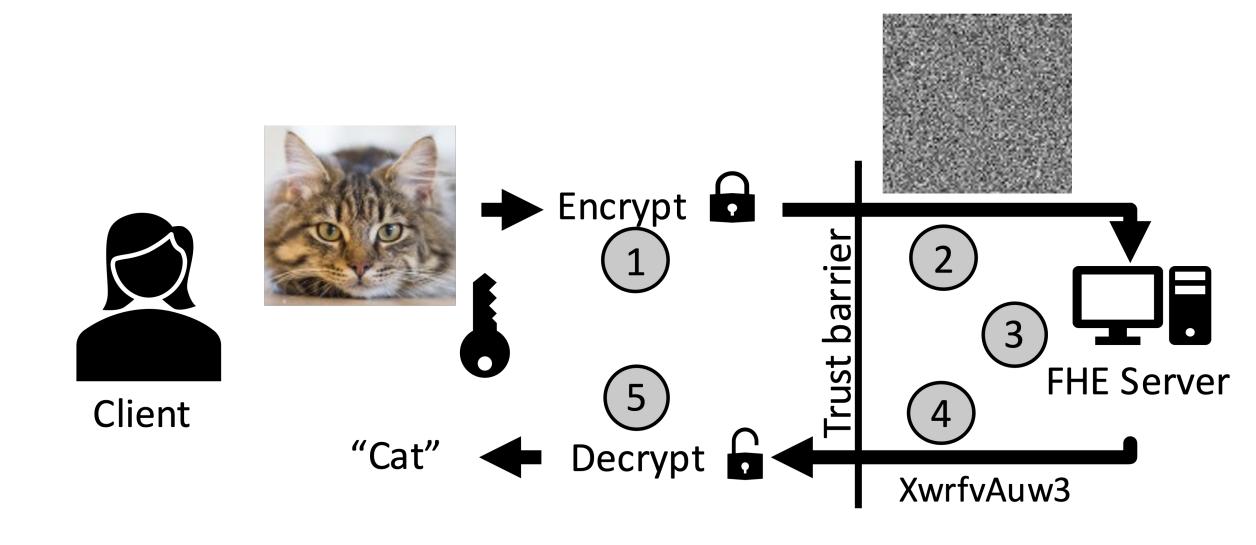
4

Ciphertext (Ct) ct.1 ct.0 Plaintext Secret 5.398 Scale (S) key 3.141 N = 2n2.721 Encrypt nRandom noise 6.465 W $\operatorname{\mathsf{mod}} \overline{q_{R-1}}$ $\mathsf{mod}\ q_0 \ \mathsf{mod}\ q_1$ • • • $w = \log_2 Q$



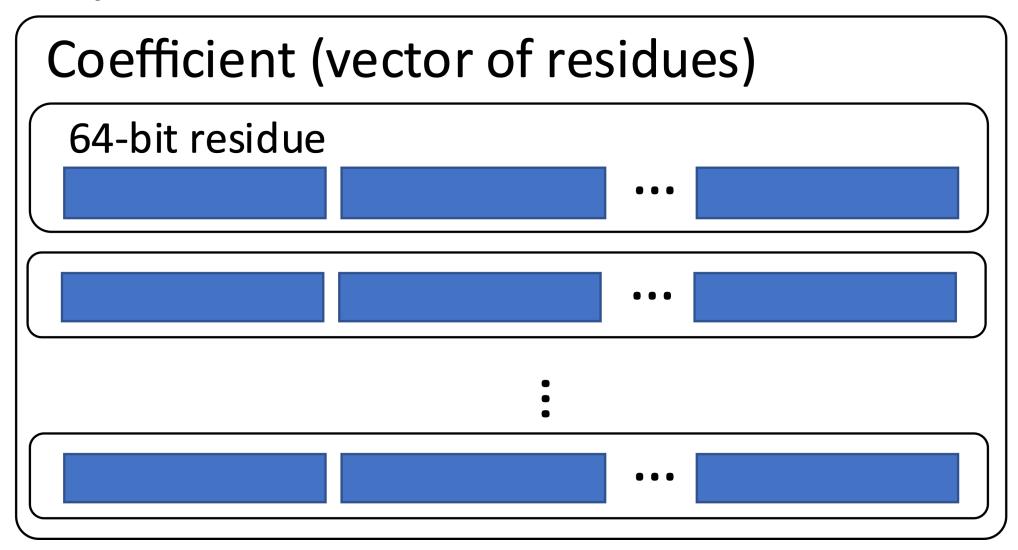


>80% of compute for keyswitching!



Old Polynomial Layout

Polynomial (vector of RnsInt's)



New Polynomial Layout

Polynomial (vector of residue polynomials)

