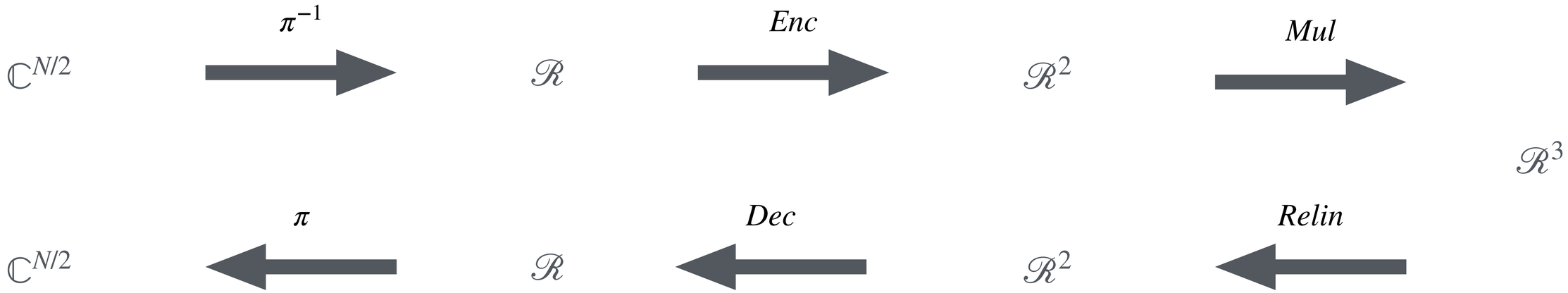
Encodage en vecteurs complexes

Paradigme Single Instruction Multiple Data (SIMD)

$$\mathscr{R} = \mathbb{Z}_q[X]/(X^N + 1)$$



$$\begin{pmatrix} a(\zeta_1) \\ \vdots \\ a(\zeta_{N/2}) \end{pmatrix} \odot \begin{pmatrix} b(\zeta_1) \\ \vdots \\ b(\zeta_{N/2}) \end{pmatrix} = \begin{pmatrix} a(\zeta_1) \cdot b(\zeta_1) \\ \vdots \\ a(\zeta_{N/2}) \cdot b(\zeta_{N/2}) \end{pmatrix} \overset{\tau}{\Longleftrightarrow} \begin{aligned} a(x) &= (a_0 + \ldots + a_{N-1}X^{N-1}) \\ \times\, b(x) &= (b_0 + \ldots + b_{N-1}X^{N-1}) \end{aligned}$$

Bootstrapping CKKS

Original bootstrapping [CHKKS18]

- [CKKS17] Permet d'évaluer des circuits arithmétiques finis
  - Chaque multiplication consomme un "niveau"