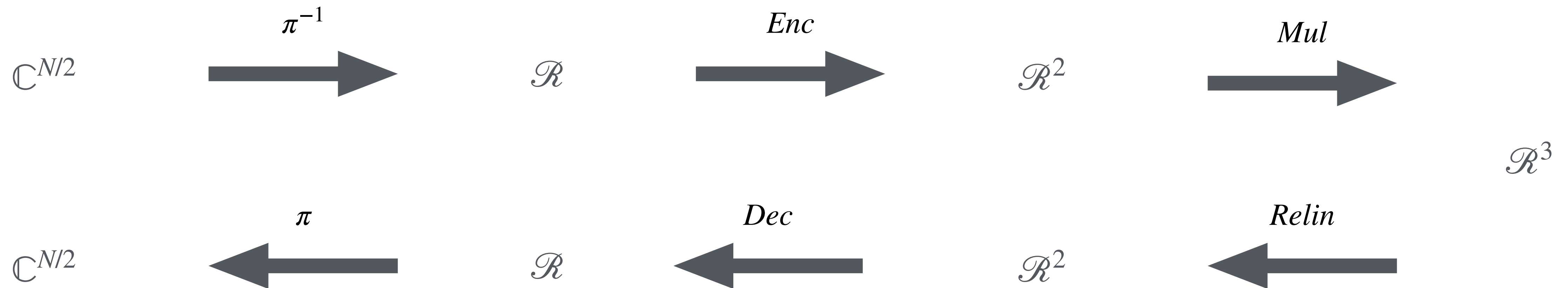


Encodage en vecteurs complexes

Paradigme Single Instruction Multiple Data (SIMD)

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



$$\begin{pmatrix} a(\zeta_1) \\ \vdots \\ a(\zeta_{N/2}) \end{pmatrix} \odot \begin{pmatrix} b(\zeta_1) \\ \vdots \\ b(\zeta_{N/2}) \end{pmatrix} = \begin{pmatrix} a(\zeta_1) \cdot b(\zeta_1) \\ \vdots \\ a(\zeta_{N/2}) \cdot b(\zeta_{N/2}) \end{pmatrix} \xLeftrightarrow{\tau} \begin{matrix} a(x) = (a_0 + \dots + a_{N-1}X^{N-1}) \\ \times b(x) = (b_0 + \dots + b_{N-1}X^{N-1}) \end{matrix}$$

Bootstrapping CKKS

Original bootstrapping [CHKKS18]

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