Encodage en vecteurs complexes

Paradigme Single Instruction Multiple Data (SIMD)

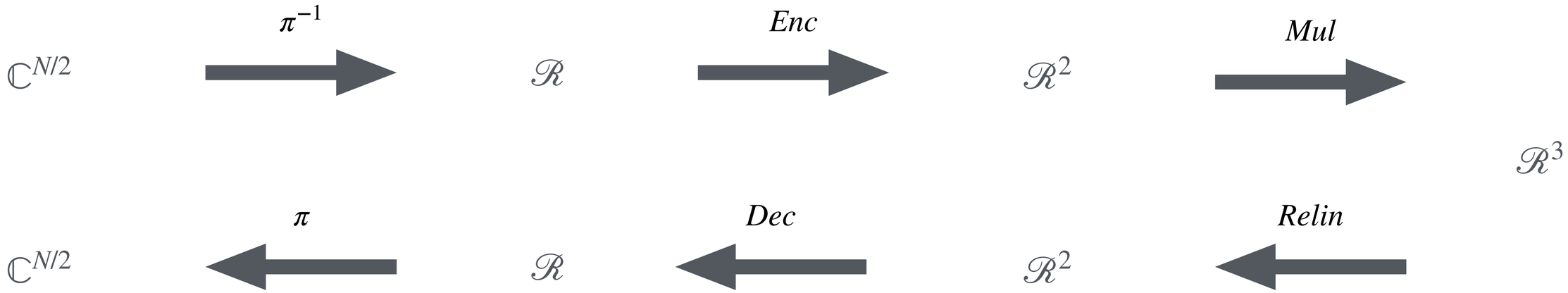
$$\mathscr{R} = \mathbb{Z}_q[X]/(X^N + 1)$$

- Un polynôme $a(x) \in \mathscr{R}$ peut être décodé dans $\mathbb{C}^{N/2}$ via $\tau : \mathscr{R} \xrightarrow{\sigma} \mathbb{C}^N \xrightarrow{\pi} \mathbb{C}^{N/2}$
- Un vecteur $z \in \mathbb{C}^{N/2}$ peut être encodé dans $\mathscr{R}$ via $\tau^{-1} : \mathbb{C}^{N/2} \xrightarrow{\pi^{-1}} \mathbb{C}^N \xrightarrow{\sigma^{-1}} \mathscr{R}$
- τ est une transformation linéaire, avec une matrice de transformation
- τ^{-1} est calculable en inversant la matrice de τ

Encodage en vecteurs complexes

Paradigme Single Instruction Multiple Data (SIMD)

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



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