Gadget Product Base2K Representation

message

noise

Vector of Polys

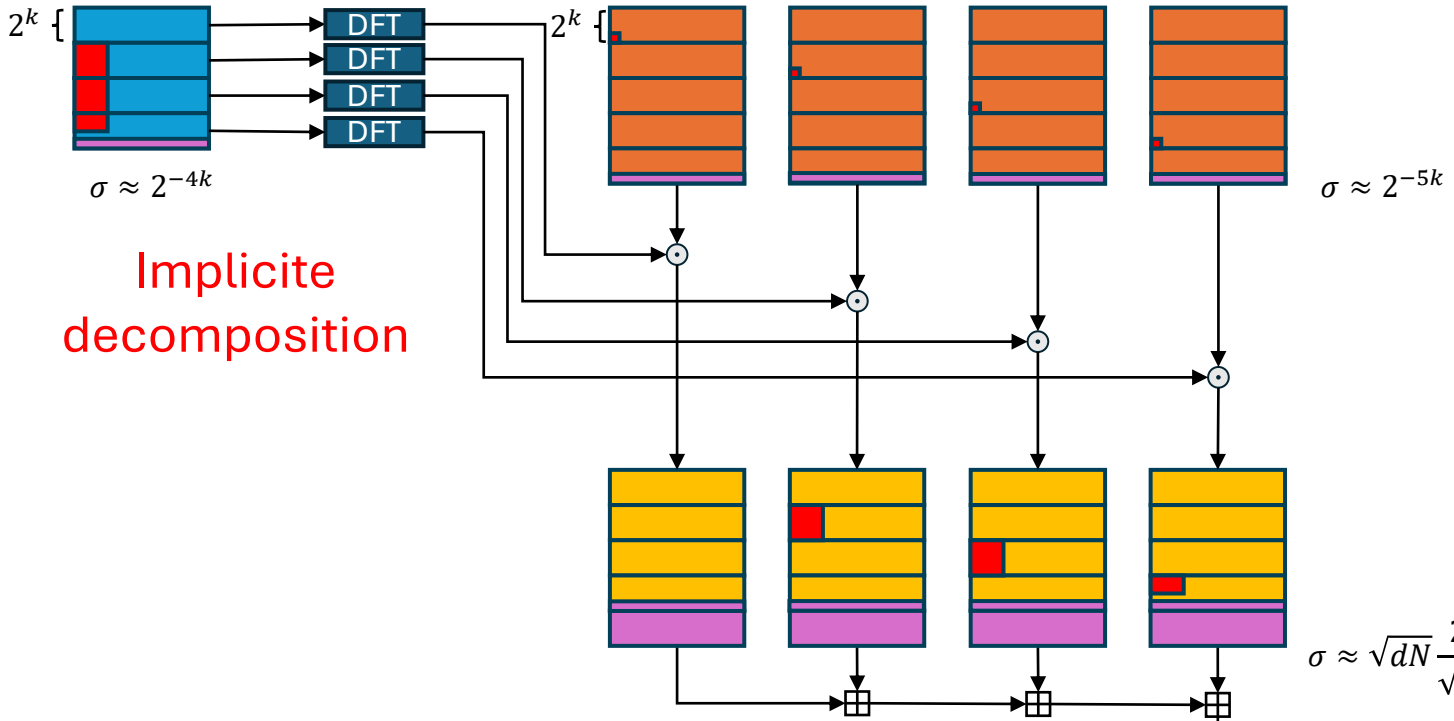
Matrix of d Polys

$\mathbb{R}_1[X]/(X^N+1)$

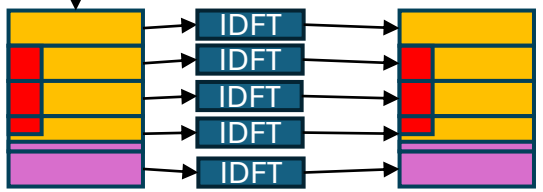
$Coeffs$

An element of the Torus (reals mod 1) is represented as a vector of polynomials with small coefficients

$Torus\ Precision$



Implicite decomposition



$$\sigma \approx \sqrt{dN}\frac{2^k}{\sqrt{12}}2^{-5k} = \sqrt{\frac{dN}{12}}2^{-4k}$$

Big Polynomials (coeffs of size 2^{2k})

Carry Propagation Small Polynomials (coeffs of size 2^k)

Truncate precision

$$\sigma \approx \left(\sqrt{\frac{dN}{12}+\frac{1}{12}}\right)\cdot 2^{-4k}$$