Chiffrement complètement homomorphe CKKS

Rappels CKKS

Chiffrement complètement homomorphe approximatif

- Originellement un schéma pour le calcul approximatif $Dec(Enc(m)) \approx m$
- On s'intéresse à la version discrète $Dec(Enc(m)) = m$
  - Correct seulement si le bruit reste sous un certain seuil
  - On encode les messages dans les bits de poids fort (à la BFV)

Message bruité [ZamaLWE]