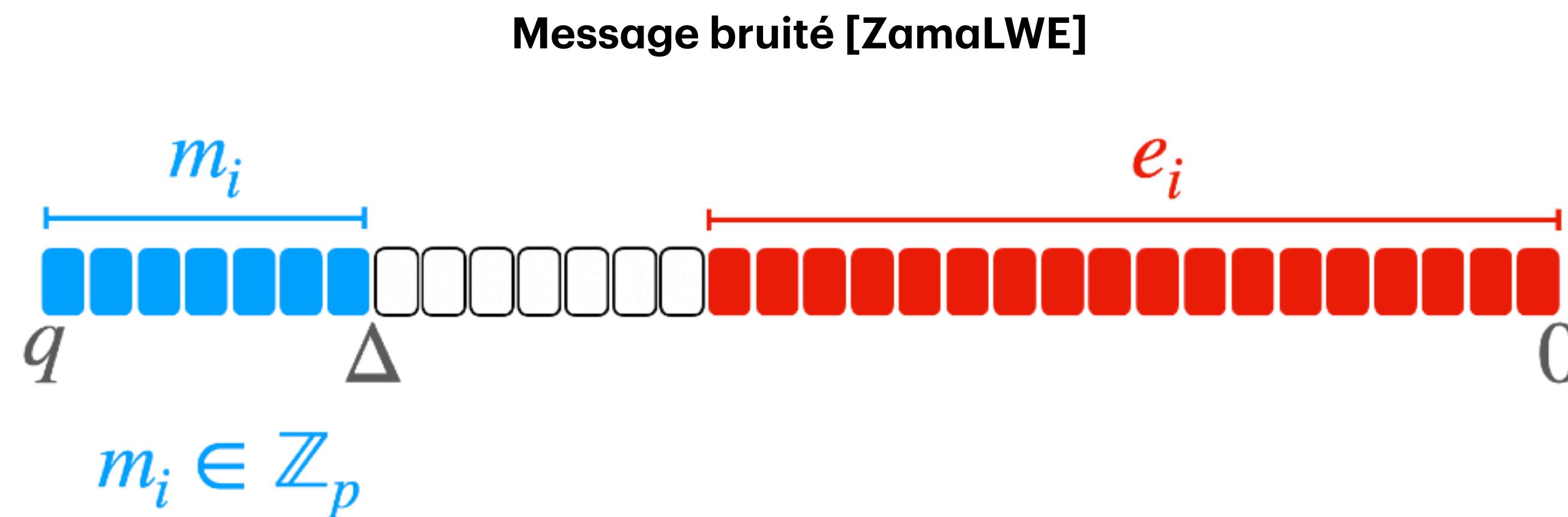


Rappels CKKS

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)



Rappels CKKS

Chiffrement complètement homomorphe approximatif

- Encodage de vecteurs complexes $a, b \in \mathbb{C}^n$ en polynômes $R_p = \mathbb{Z}_p[X]/(X^N + 1)$
 - Identifiant la multiplication polynomiale au produit de Hadamard (terme à terme)
 - Chiffrement RLWE par masquage et bruitage
 - Combinaisons linéaires pour $c \in \mathbb{C}$ "gratuites"
 - Multiplications chiffrées coûteuses
- ⇒ Évaluation (SIMD) de polynôme $P(x)$ sur un chiffré
- $$E(a) + cE(b) = E(a + cb)$$
- $$E(a) \times E(b) = E(a \odot b)$$
- $$P(E(a)) = E(P(a))$$