How is this 8us calculated?

- us is a measure unit for Frobeni**us**Map(a,n) map function in NTT domain.

Using the formular:

z ∈ C M τ −1 −−→ (mQ(X)) ∈ Q(X)/(XN + 1) bΔ·e −−−→ m(X) ∈ RQ`

where τ : zi 7→ mQ(ζi) and ~z = (zi)i∈[0,N−1], ζi = ζ 5` , ζ = exp(−2πi/4M), and [Δ·] : a → [Δ · a].

The result obtained is defined by substituting ζi for X in mQ(X) as the value of the **i-th slot**.

Considering slot rotation: assuming that the rotation by n slots is performed in mq(X),

the resultant polynomial m`Q (X) ∈ Q[X]/(XN + 1)

should preserve m`Q(ζi) = m0 Q (ζi+n).

That is, the value in the (i + n)-th slot of m`Q (X) should be the same as the one in the i-th slot of mQ(X).

Because ζi+n = ζ 5 i+n = ζ 5 n i , we need to compute m` Q (X) = mQ(X^(5 −n)) from mQ(X).