Bootstrapping: need to eval $Dec(\boxed{sk}, ct)$

- cycle: new assumption, one fixed scheme all circuits.
- laddar: security LWE, only n depends on depth. (leveled FHE)

Both cases: $Dec(sk, ct)$ has depth $O(\log \lambda)$ ← NC1

can set $q = \lambda^{O(\log \lambda)}$

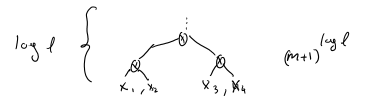
Can we do poly modulus? Yes!

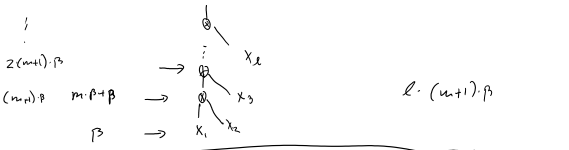
$C_1 = \underset{\text{error } \beta_1}{Enc_{sk}(x_1)}$, $C_2 = \underset{\text{error } \beta_2}{Enc_{sk}(x_2)}$

$C^+ = C_1 + C_2$ error $\beta_1 + \beta_2$

$C^\times = C_1 \cdot G^{-1}(C_2)$ error $\beta_1 \cdot m + x_1 \cdot \beta_2$ ←

Ex. Let $C_1, \dots, C_\ell$: $C_i = Enc_{sk}(x_i)$





By careful anal of Dec, can do it with poly error.

NC1 → perm branching prog → rest. straight-line progs.

- load input bit / constant to register

"$r_i := x_j$" or "$r_i := 0$"

- permute: "$r_i := r_j \cdot x_k + r_\ell (1 - x_k)$"

$\beta^4 \longrightarrow (\beta^4 \cdot x_k + m\beta) + (\beta^4 (1 - x_k) + m\beta)$

$= \beta^4 + 2 \cdot m \cdot \beta$

[BV 13?]