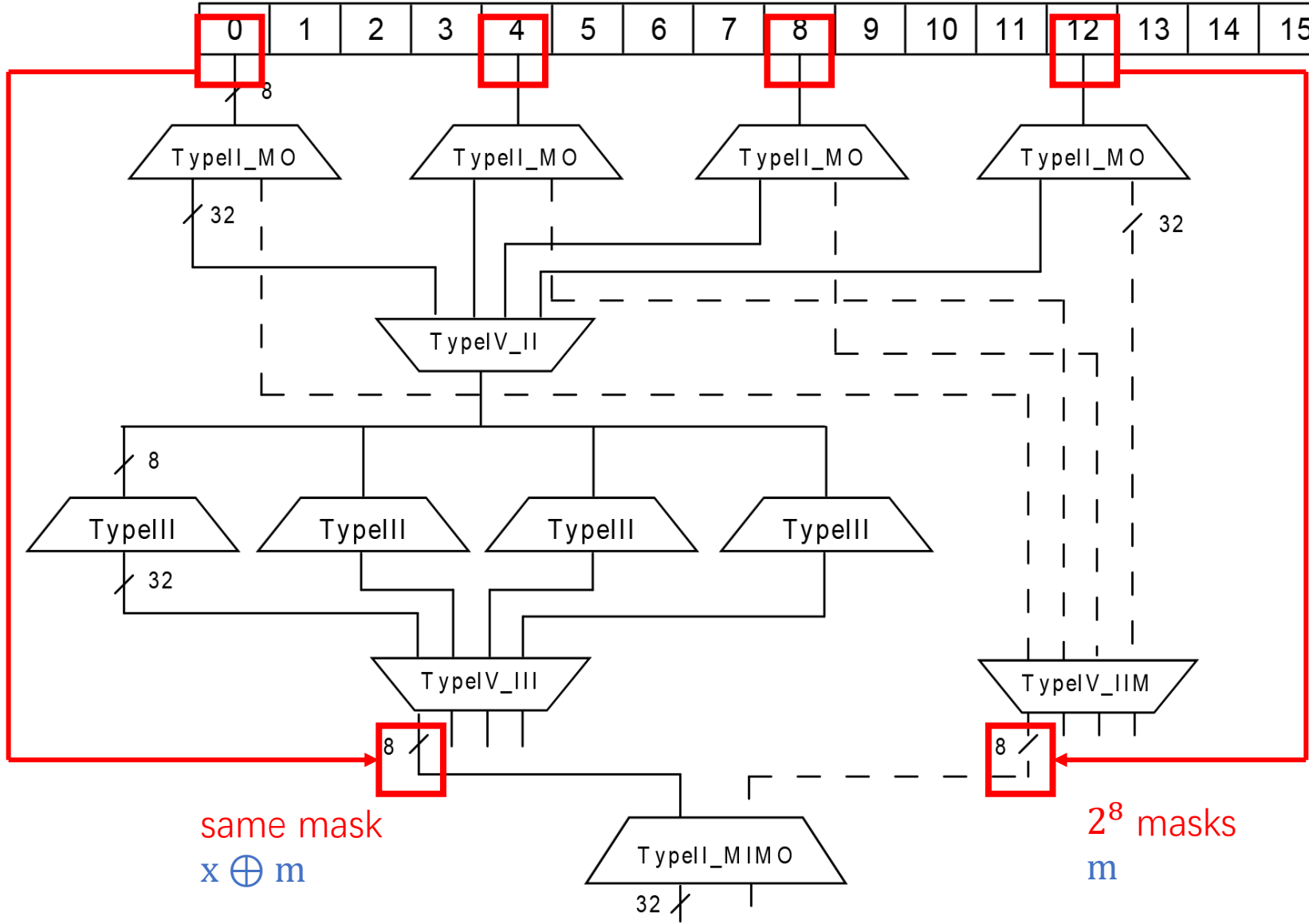
nearly 2^8 chosen plaintexts $(x_0, x_1, 0,0) \in W$



2^{16} plaintexts $(x_0, x_1, 0,0)$

② The masks of the 1st round outputs are identical to each other,

① Choosing the plaintexts which have the same mask.

same mask $x \oplus m$

2^8 masks m