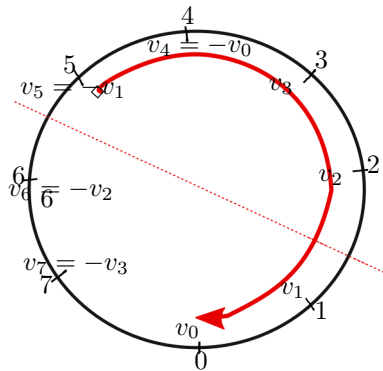


TLWE ciphertext

$$N = 4, \text{ mod } X^{2N} - 1$$



$$ACC_0 = v_0X^0 + v_1X + \dots + v_7X^7$$