$$(a_3 X^3 + a_2 X^2 + a_1 X^1 + a_0 X^0) * (b_3 X^3 + b_2 X^2 + b_1 X^1 + b_0 X^0) \quad MOD(X^4 - \lambda)$$

$$= a_3 b_3 X^6 + (a_3 b_2 + a_2 b_3) X^5 + (a_3 b_1 + a_2 b_2 + a_1 b_3) X^4$$

$$+ (a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3) X^3 + (a_2 b_0 + a_1 b_1 + a_0 b_2) X^2 + (a_1 b_0 + a_0 b_1) X^1 + a_0 b_0 X^0 \quad MOD(X^4 - \lambda)$$

$$= X^4 (a_3 b_3 X^2 + (a_3 b_2 + a_2 b_3) X^1 + (a_3 b_1 + a_2 b_2 + a_1 b_3) X^0)$$

$$+ (a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3) X^3 + (a_2 b_0 + a_1 b_1 + a_0 b_2) X^2 + (a_1 b_0 + a_0 b_1) X^1 + a_0 b_0 X^0 \quad MOD(X^4 - \lambda)$$

$$= (X^4 - \lambda + \lambda)(a_3 b_3 X^2 + (a_3 b_2 + a_2 b_3) X^1 + (a_3 b_1 + a_2 b_2 + a_1 b_3) X^0)$$

$$+ (a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3) X^3 + (a_2 b_0 + a_1 b_1 + a_0 b_2) X^2 + (a_1 b_0 + a_0 b_1) X^1 + a_0 b_0 X^0 \quad MOD(X^4 - \lambda)$$

$$= (a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3) X^3 + (\lambda a_3 b_3 + a_2 b_0 + a_1 b_1 + a_0 b_2) X^2 + (\lambda (a_3 b_2 + a_2 b_3) + a_1 b_0 + a_0 b_1) X^1 + (\lambda (a_3 b_1 + a_2 b_2 + a_1 b_3) + a_0 b_1) X^0$$