ECC Cryptography

The elliptic curve is defined as:

$$y^2 = x^3 + 2x + 7 \pmod{31} \tag{1}$$

The private key is:

$$m = 8 \quad \text{(private key)} \tag{2}$$

The initial point is:

$$P = (2, 9) \quad \text{(initial point)} \tag{3}$$

The public key is computed as:

$$Q = mP \quad \text{(public key)} \tag{4}$$

Encryption

For encryption, we choose a random key k for each encryption. Then:

$$C_1 = kP \tag{5}$$

$$M_c = M + S_x \pmod{p} \tag{6}$$

where:

$$S = kQ \quad \text{and} \quad S_x \text{ is the } x\text{-component of } S. \tag{7}$$

Decryption

To decrypt the ciphertext (C_{1x}, C_{1y}, M_c):

$$S = mC_1 = m(C_{1x}, C_{1y}) \tag{8}$$

$$M = M_c - S_x \pmod{p} \tag{9}$$

Note

Important: In this case, we only use S_x as a shared secret to reduce the computation.