

Note that we have $P = (P_x, P_y)$ and $Q = (Q_x, Q_y) = 2P$. We'd like to find (some? all? of the) elliptic curve parameters, p, a, b . Possibly only p .

Define $\gamma = \frac{3P_x^2 + a}{2P_y}$.

Then, from the definition of elliptic curve addition,

$$\begin{aligned} Q_x &\equiv \gamma^2 - 2P_x && \text{mod } p^k \\ \gamma^2 &\equiv Q_x + 2P_x && \text{mod } p^k \quad (1) \\ Q_y &\equiv \gamma(P_x - Q_x) - P_y && \text{mod } p^k \\ \gamma &\equiv \frac{Q_y + P_y}{P_x - Q_x} && \text{mod } p^k \quad (2) \end{aligned}$$

Subbing (2) into (1):

$$\begin{aligned} \left(\frac{Q_y + P_y}{P_x - Q_x}\right)^2 &\equiv Q_x + 2P_x && \text{mod } p^k \\ (Q_y + P_y)^2 &\equiv (Q_x + 2P_x)(P_x - Q_x)^2 && \text{mod } p^k \\ 0 &\equiv (Q_y + P_y)^2 - (Q_x + 2P_x)(P_x - Q_x)^2 && \text{mod } p^k \\ np^k &= (Q_y + P_y)^2 - (Q_x + 2P_x)(P_x - Q_x)^2 \end{aligned}$$

Note that we can compute np^k since we have all of the variables on the RHS. We find $p = 12654803915193133223$.

Plugging this into γ , we can find

$$\begin{aligned} \gamma &= \frac{Q_y + P_y}{P_x - Q_x} \quad (2) \\ \gamma &= \frac{3P_x^2 + a}{2P_y} \end{aligned}$$

$$2P_y\gamma = 3P_x^2 + a$$

$$a = 2P_y\gamma - 3P_x^2$$

Finally, by definition of EC,

$$y^2 = x^3 + ax + b \quad \text{mod } p^4$$

$$b = P_y^2 - P_x^3 - aP_x$$