ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

(2 pages)

Addition Law on E:

Let $(x_1, y_1), (x_2, y_2)$ be two arbitrary points on an elliptic curve $E : y^2 \equiv x^3 + bx + c$. Then

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3) = \big(m^2 - x_1 - x_2,\ \ m(x_1 - x_3) - y_1\big),$$

where

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } (x_1, y_1) \neq (x_2, y_2), \\ \\ \frac{3x_1^2 + b}{2y_1} & \text{if } (x_1, y_1) = (x_2, y_2). \end{cases}$$

Remark: *When considering an elliptic curve* $E \pmod p$*, for a prime* p*, we replace* $\frac{y_2 - y_1}{x_2 - x_1}$ *by* $(y_2 - y_1) \cdot (x_2 - x_1)^{-1} \pmod p$ *and similarly for* $\frac{3x_1^2 + b}{2y_1}$.

ECC KEY EXCHANGE

Public Information:

$p =$ large prime. Two integers $1 < b, c < p$.

$E : y^2 \equiv x^3 + bx + c \pmod p$, $\qquad \big($an elliptic curve $(\text{mod } p)\big)$.

$Q = (x_0, y_0)$ a point on $E \pmod p$ with $1 < x_0, y_0 < p$, i.e., $y_0^2 \equiv x_0^3 + bx_0 + c \pmod p$.

Elliptic Curve Key Exchange Protocol:

Alice's Private Key: $\boxed{1 < \alpha < p.}$

Alice's Public Key: $\alpha\, Q := \underbrace{Q \oplus \ \cdots\ \oplus Q}_{\alpha \text{ ECC additions}}$

Bob's Private Key: $\boxed{1 < \beta < p.}$

Bob's Public Key: $\beta\, Q := \underbrace{Q \oplus \ \cdots\ \oplus Q}_{\beta \text{ ECC additions}}$

$\boxed{\textbf{Shared Secret = Exchanged Key } = \ \alpha\beta\, Q.}$

Toy Example: $p = 17, \quad E : y^2 \equiv x^3 + x + 6 \pmod{17}, \quad Q = (2, 4).$

Alice's Private Key $= 2$

Alice's Public Key $= (2, 4) \oplus (2, 4) = (x_3, y_3)$, where we compute x_3, y_3 as follows:

$$m \equiv (3 \cdot 2^2 + 1) \cdot (2 \cdot 4)^{-1} \equiv 8 \pmod{17},$$

$$x_3 \equiv 8^2 - 2 - 2 \equiv 9 \pmod{17}, \qquad y_3 \equiv 6(2 - 0) - 4 \equiv 8 \pmod{17},$$

$$\boxed{\textbf{Alice's Public Key} = (2, 4) \oplus (2, 4) = (9, 8)}$$

Bob's Private Key $= 3$

Bob's Public Key $= (2, 4) \oplus (2, 4) \oplus (2, 4) = (9, 8) \oplus (2, 4) = (x_3, y_3)$, where we compute x_3, y_3 as follows:

$$m \equiv (4 - 8) \cdot (2 - 9)^{-1} \equiv 3 \pmod{17},$$

$$x_3 \equiv 3^2 - 9 - 2 \equiv 15 \pmod{17}, \qquad y_3 \equiv 3(9 - 15) - 8 \equiv 8 \pmod{17},$$

$$\boxed{\textbf{Bob's Public Key} = (2, 4) \oplus (2, 4) \oplus (2, 4) = (15, 8)}$$

$$\boxed{\textbf{Shared Secret = Exchanged Key} = 6(2, 4) = (15, 8) \oplus (15, 8) = (3, 6)}$$