Camlin Page
Date / /

Point Addition

Let $P(x_1, y_1)$ & $Q(x_2, y_2)$ be 2 points on $E(\mathbb{F}_{2^m})$
Let $R = P + Q = (x_3, y_3)$
Now, first lets find slope (λ) =

$$= \frac{y_2 - y_1}{x_2 - x_1}$$

$$\boxed{\lambda = \frac{y_2 + y_1}{x_2 + x_1}} \quad ① \qquad \left[-a = a \ \forall a \in \mathbb{F}_{2^m}\right]$$

Now, we know $y = \lambda x + c$ ②
Sub ② in $E(\mathbb{F}_{2^m})$

$$\Rightarrow (\lambda x + c)^2 + x(\lambda x + c) = x^3 + ax^2 + b$$

~~$(\lambda x + c)^2 + x(\lambda x + c) = x^3 + ax^2 + b$~~

$$\Rightarrow \lambda^2 x^2 + 2\lambda c x + c^2 + \lambda x^2 + xc = x^3 + ax^2 + b$$

$$x^3 + (a - \lambda^2 - \lambda)x^2 + (2\lambda c - c)x + b - c^2 = 0$$

[As $-a = a$ for $\forall a \in \mathbb{F}_{2^m}$]

$$\Rightarrow x^3 + (a + \lambda^2 + \lambda)x^2 + (2\lambda c + c)x + b + c^2 = 0$$

As per polynomial relation rule (x_1, x_2 & x_3 as roots)

$$\Rightarrow -(a + \lambda^2 + \lambda) = x_1 + x_2 + x_3$$

$$\Rightarrow -x_3 = \lambda^2 + \lambda + a + x_1 + x_2$$

$$\boxed{\therefore x_3 = \lambda^2 + \lambda + x_1 + x_2 + a} \quad ③ \qquad \left[\text{as } \underset{\forall a \in \mathbb{F}_{2^m}}{a = -a}\right]$$

Now, $y_1 = \lambda x_1 + c \Rightarrow c = y_1 - \lambda x_1$
& $x_3 + y_3 = \lambda x_3 + c$ [As $P(x_3, x_3 + y_3)$ is on the same line]
$\Rightarrow$ Same λ & c

Now, substituting c

$$x_3 + y_3 = \lambda x_3 + y_1 - \lambda x_1$$

$$y_3 = \lambda x_3 + y_1 - \lambda x_1 - x_3$$

$$y_3 = \lambda x_3 + y_1 + \lambda x_1 + x_3 \qquad [-a = a \ \forall a \in \mathbb{F}_{2^m}]$$

$$\boxed{y_3 = \lambda(x_3 + x_1) + x_3 + y_1} \quad \text{④}$$

From ①, ③ & ④, All Derivations are proved.

Point Doubling

Now, $y^2 + xy = x^3 + ax^2 + b$

Applying $\frac{d}{dx}$ on both sides

$$2y.dy + y.dx + x.dy = 3x^2.dx + 2ax.dx$$
$$2y.dy + x.dy = 3x^2.dx + 2ax\,dx - y\,dx$$

$$dy(2y + x) = dx(3x^2 + 2ax - y)$$

$$\boxed{\lambda = \frac{dy}{dx} = \frac{3x^2 + 2ax - y}{2y + x}} \quad \text{①}$$

Since $P(x_1, y_1) + P(x_1, y_1) = 2P(x_3, y_3)$ is also addition,

$$\boxed{x_2 = \lambda^2 + \lambda + 2x_1 + a}$$

& $$\boxed{y_2 = \lambda(x_2 + x_1) + x_2 + y_1}$$