# Extension Fields $GF(2^n)$

$$GF(2^n) = \{ a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{Z}_2 = \{0,1\},\ i = 0,1,\ldots,n-1 \}$$

A polynomial of deg $n-1$ represents an $n$-bit word

Ex. $x^4 + x^3 + x + 1$

11011

$$GF(2^3) = \{0,\ 1,\ x,\ x^2+1,\ x^2,\ x^2+x,\ x^2+x+1,\ x+1\}$$

000, 001, 010, 101, 100, 110, 111, 011

1. Addition: Let $P_1(x)$ & $P_2(x) \in GF(2^n)$ where

$$P_1(x) = \sum_{i=0}^{n-1} a_i x^i, \quad P_2(x) = \sum_{i=0}^{n-1} b_i x^i$$

$$P_1(x) + P_2(x) = \sum_{i=0}^{n-1} c_i x^i \quad \text{where } c_i = (a_i + b_i) \bmod 2,\ i = 0,1,\ldots,n-1$$

Additive Identity $= 0$.

Additive Inverse of $p(x) = p(x) \Rightarrow (p(x))^{-1} = p(x)$

2. Multiplication:

$x^2+1$ - irreducible in $\mathbb{R}$

$x^2+1$ - Reducible in $(\mathbb{C},+,\cdot)$ $(x+i)(x-i)$

Q. What modulo operation we should use?

Let modulo $(x^2+1)$ in $GF(2^2)$

$(x+1) \in GF(2^2)$

Now,
$$\begin{aligned}(x+1)^2 \bmod (x^2+1) &= (x+1)(x+1) \bmod (x^2+1)\\ &= (x^2+2x+1) \bmod (x^2+1)\\ &= (x^2+1) \bmod (x^2+1)\\ &= 0\end{aligned}$$

Now, let $p(x) = (x+1)^{-1} \bmod (x^2+1)$

$p(x)\,(x+1) \bmod (x^2+1) = 1$ (Mult. identity)

$p(x)\,\underbrace{(x+1)(x+1) \bmod (x^2+1)} = (x+1) \Rightarrow \underbrace{0 = x+1}$

This is absurd

$\Rightarrow (x+1)^{-1}$ does not exist.

$(x+1)$ is a factor of $x^2+1$ in $GF(2^2)$

$\Rightarrow x^2+1$ is reducible in $GF(2^2)$

| Deg | Irreducible Polynomial over $\underline{\mathbb{Z}_2}$ |
| --- | --- |
| 1 | $(x+1)$, $x$ |
| 2 | $x^2+x+1$ |
| 3 | $x^3+x^2+1$, $x^3+x+1$ |
| 4 | $x^4+x^3+x^2+x+1$, $x^4+x^3+1$, $x^4+\underline{x+1}$. |

Now, $\underset{\sim\sim}{GF(2^3)}$, $+$, mod $(x^3+x+1)$

$$x^3+x+1 \,\big)\, x^3 \,(\, 1$$
$$\underline{x^3 \underset{-}{+} x \underset{-}{+} 1}$$
$$\underline{-x-1}$$
$$= x+1$$

Non-zero elements of $GF(2^3)$

$\{\underline{1}, \underline{x}, \underline{x^2}, \underline{x+1}, x^2+x, x^2+1, x^2+x+1\}$

$\underline{x^0} = 1$, $x^1 = x$, $x^2 = x^2$, $x^3 = x+1 \mod (x^3+x+1)$

$x^4 = x^3 \cdot x = x^2+x$, $x^5 = x^3+x^2 = x^2+x+1$

$x^6 = x^3+x^2+x = \underline{x+1} + x^2 + \underline{x} = x^2+1$

$x$ is a generator of $\underline{GF(2^3)}$, mod $(x^3+x+1)$

$GF(2^3) = \{0, 1, x, x^2, x^3, x^4, x^5, x^6\}$ operations. Addition
Mult mod.
$(x^2+x+1)$

## Elliptic Curves over $GF(2^n)$

$$y^2 + xy = x^3 + ax^2 + b \quad \text{where } b \neq 0$$

& where, $x, y, a, b$ are polynomials in $\underline{GF(2^n)}$.

$$E_{2^n}(a,b) = \{(x,y) \mid x, y \in GF(2^n) \text{ s.t } y^2+xy = x^3+ax^2+b\}$$

**Addition.** 1. If $P = (x_1, y_1)$, $Q = (x_2, y_2)$ & $Q = -P$ & $Q \neq P$

Then $\cdot P+Q = R\,(x_3, y_3)$ is given by

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \quad , \quad y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

Where $\lambda = \dfrac{y_2 + y_1}{x_2 + x_1}$

2. If $P = Q$ then $P + Q = P + P = 2P = R\ (x_3, y_3)$

$$x_3 = \lambda^2 + \lambda + a \quad , \quad y_3 = x_1^2 + (\lambda + 1)x_3 \quad \text{where } \lambda = \frac{x_1 + y_1}{x_1}$$

## Elliptic Curve Cryptography

1 Elliptic Curve Diffie-Hellman Key Exchange:

Public Parameters : $E_q(a,b)$ : Elliptic curve with parameters $a, b$ & $q$, where $q$ is a prime or of the form $2^n$.

$G$ : Point on elliptic curve whose order is very Large

**Alice**

$a = K_{prA} \in \{2, 3, \ldots, |E_q(a,b)| - 1\}$

$A = K_{pubA} = a \cdot G = (x_A, y_A)$

$\xrightarrow{A}$

B $\xleftarrow{B}$

$K = \underline{aB} = (x_{AB}, y_{AB})$

**Bob**

$b = K_{prB} \in \{2, 3, \ldots, |E_q(a,b)| - 1\}$

$B = K_{pubB} = b \cdot G = (x_B, y_B)$

A

$K = \underline{bA} = (x_{AB}, y_{AB})$

$$\boxed{aB = a(b \cdot G) = b(aG) = \underline{\underline{bA}}}$$

## 2. Encryption & Decryption using Elliptic Curves.

Alice | Bob

Key Generation:

1. Bob chooses $E_q(a,b)$ over $GF(P)$ or $GF(2^n)$
2. " " a point on the curve $E_q(a,b)$ $e_1 = (x_1, y_1)$
3. Choose an integer $d$ (Private key)
4. Compute $e_2 = d \times e_1$

Public ← $(e_1, e_2, E_q(a,b))$

Encryption:

1. Alice choose an integer $r$
2. Alice select a point $P$ one the curve as her plaintext
3. $C_1 = r \times e_1$ , $C_2 = P + r \times e_2$

$(C_1, C_2)$ — Ciphertext → $(C_1, C_2)$

Decryption:

$$
\begin{aligned}
C_2 - d \times C_1 &= P + r \times e_2 - d \times r \times e_1 \\
&= P + (r \times d \times e_1) - (r \times d \times e_1) \\
&= P + 0 \\
&= P \quad (\text{Plaintext})
\end{aligned}
$$