· 전체 S-BOX

$\zeta \in GF((2^4)^2)$일 때, $\zeta = z_1\gamma + z_0$

polynomial basis → 기약다항식 $P(x) = x^2 + Ax + B$

γ는 $P(x)$의 근. $\gamma^2 + A\gamma + B$.

$\zeta^{-1} = \delta = D_1\gamma + D_0$

$\zeta \cdot \delta = 1 = D_1 z_1 \gamma^2 + (D_1 z_0 + D_0 z_1)\gamma + D_0 z_0$ ($\gamma^2 = A\gamma + B$ 대입)

$\Rightarrow 1 = (D_1 z_0 + D_0 z_1 + AD_1 z_1)\gamma + (D_0 z_0 + BD_1 z_1)$ 계수 비교.

$1 = \quad 0 \cdot \gamma \quad + \quad 1$

$$\begin{cases} D_1 z_0 + D_0 z_1 + AD_1 z_1 = 0 & \cdots ① \\ D_0 z_0 + BD_1 z_1 = 1 & \cdots ② \end{cases}$$

① → $D_1(z_0 + Az_1) = D_0 z_1 \Rightarrow D_1 = D_0 z_1 (z_0 + Az_1)^{-1} \cdots ③$

$\Rightarrow D_0 = D_1 z_1^{-1}(z_0 + Az_1) \cdots ④$

③을 ②에 대입. $\Rightarrow D_0 z_0 + B(D_0 z_1(z_0 + Az_1)^{-1}) z_1 = 1$

$\rightarrow D_0(z_0 + Bz_1^2(z_0 + Az_1)^{-1}) = 1$

$\rightarrow \boxed{D_0 = (z_0 + Az_1) \cdot F^{-1}}$

④를 ②에 대입 $\Rightarrow D_1 z_1^{-1} z_0 (z_0 + Az_1) + BD_1 z_1 = 1$

$\rightarrow D_1 z_1^{-1}(z_0^2 + Az_1 z_0 + Bz_1^2) = 1$

$\rightarrow \boxed{D_1 = z_1 \cdot F^{-1}}$

→ $F = z_0^2 + Az_1 z_0 + Bz_1^2$

$(z_1\gamma + z_0)^{-1} = D_1\gamma + D_0$ $\quad \begin{cases} D_1 = z_1 \cdot F^{-1} \\ D_0 = (z_0 + Az_1) \cdot F^{-1} \end{cases}$, $F = z_0^2 + Az_1 z_0 + Bz_1^2$

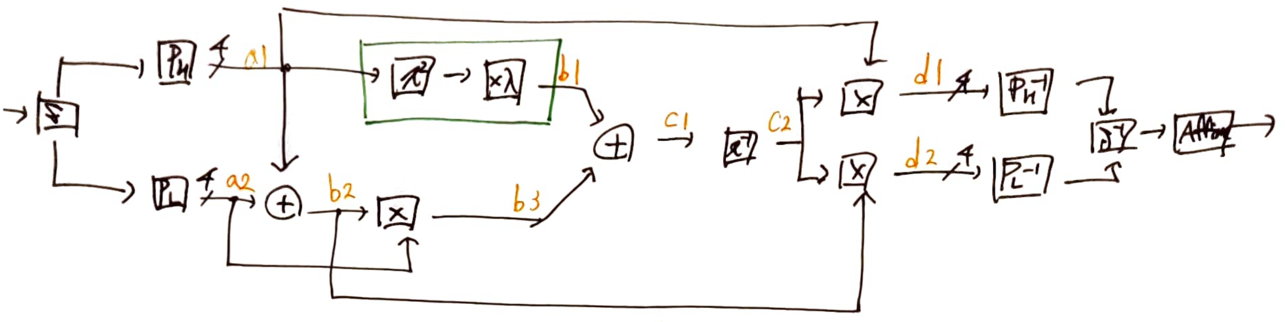
z_1, z_0를 각각 P_H, P_L, $A = 1, B = \lambda$로 둔다면.

γ는 x로 둔다면,

$(P_H x + P_L)^{-1} = D_1 x + D_0$

$$= \underbrace{P_H(P_H^2\lambda + (P_H + P_L)P_L)^{-1}}_{\hookrightarrow P_H^{-1}} x + \underbrace{(P_H + P_L)(P_H^2\lambda + (P_H + P_L)P_L)^{-1}}_{\hookrightarrow P_L^{-1}}$$

⇒ S-BOX 분해.



$\boxed{x^{-1}}$: $GF((2^4)^2)$ 상의 역원.

$\boxed{\delta}$: 체 변환.

$\boxed{\delta^{-1}}$: 체 역변환

$\boxed{\text{Affine}}$: 아핀변환

$\boxed{\times}$: $GF((2^4)^2)$ 의 유한체 곱셈 연산기.

$\boxed{x^2} \rightarrow \boxed{\times\lambda}$ 단순화.

$$\begin{cases} GF(2) \Rightarrow GF(2^2), & P_0(x) = x^2+x+1 \\ GF(2^2) \Rightarrow GF((2^2)^2), & P_1(x) = x^2+x+\phi \\ GF((2^2)^2) \Rightarrow GF(((2^2)^2)^2), & P_2(x) = x^2+x+\lambda \end{cases}$$

$\phi = 10$, $\lambda = 1100$ 선택.

$\Rightarrow$ $\phi = X$, $\lambda = (X+1)Y$

Input 8bit $\Rightarrow$ $\underbrace{((ax+b)Y + (cx+d))}_{\hookrightarrow P_H} Z + \underbrace{((ex+f)Y + gx+h)}_{\hookrightarrow P_L}$

$$\begin{cases} Z^2+Z+\lambda = 0 \\ Y^2+Y+\phi = 0 \\ X^2+X+1 = 0 \end{cases} \Rightarrow \begin{cases} Z^2 = Z+\lambda = Z+(X+1)Y = Z+Y+XY \\ Y^2 = Y+\phi = Y+X \\ X^2 = X+1 \end{cases}$$

i) $P_n \to \boxed{x^2} \to$

2a = a+a
↳ 2n 소멸 → 0
∴ 2a 꼴은 0으로

$$((ax+b)y + (cx+d))^2$$

$$= (ax+b)^2y^2 + \cancel{2(ax+b)y(cx+d)}^{\to 0} + (cx+d)^2$$

$$= (a^2x^2 + \cancel{2ab}x + b^2)(y+x) + c^2x^2 + \cancel{2cd}x + d^2$$

$$= (a(x+1)+b)(y+x) + c(x+1)+d$$

$$= (ax+a+b)(x+y) + cx+c+d$$

$$= ax^2 + ax + bx + axy + ay + by + cx + c + d$$

$$= a(x+1) + ax + bx + axy + ay + by + cx + c + d$$

$$= \cancel{2ax} + a + bx + axy + ay + by + cx + c + d$$

$$= y(ax+a+b) + (b+c)x + a+c+d$$

ii) $\to \boxed{\times \lambda} \to$

$$((ax+a+b)y + (b+c)x + a+c+d) \times \underbrace{(x+1)y}_{\lambda}$$

$$= (ax+a+b)(x+1)y^2 + (b+c)(x^2+x)y + (a+c+d)(x+1)y$$

$$= (ax+a+b)(x+1)(x+y) + (b+c)(\cancel{2x}+1)y + (a+c+d)(xy+y)$$

$$= \underbrace{(ax+a+b)(x+1)(x+y)}_{①} + \underbrace{(b+c)y + (a+c+d)(xy+y)}_{②}$$

① ⇒ $(ax+a+b)(x^2+x+xy+y) = (ax+a+b)(x+1+x+xy+y)$

$= (ax+a+b)(\cancel{2x}+1+xy+y) = (ax+a+b)(xy+y+1)$

$= ax^2y + axy + bxy + axy + ay + by + ax + a + b$

$= ax^2y + \cancel{2axy} + bxy + ay + by + ax + a + b$

$= a(x+1)y + bxy + ay + by + ax + a + b = axy + ay + bxy + ay + by + ax + a + b$

$= axy + \cancel{2ay} + bxy + by + ax + a + b = axy + bxy + by + ax + a + b = \underbrace{y(ax+bx+b) + ax + a + b}_{③}$

③+② ⇒ $y(ax+bx+b+b+c+ax+cx+dx+a+c+d) + ax+a+b$

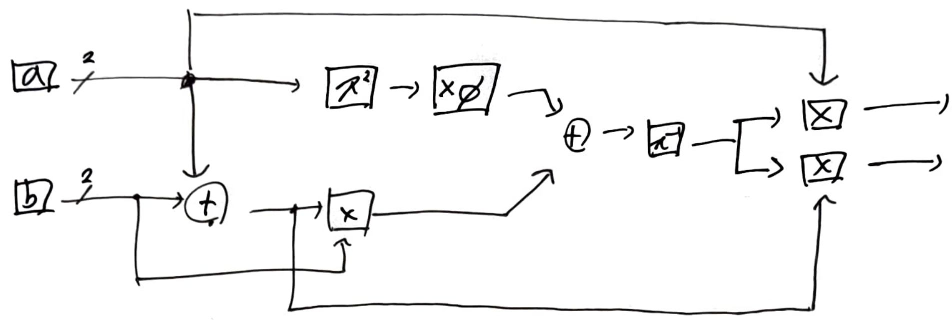
$= y(\cancel{2ax} + bx + cx + dx + \cancel{2b} + a + \cancel{2c} + d) + ax + a + b$

$= y((b+c+d)x + a+d) + ax + a + b$

⇒ $((b+c+d)x + (a+d))y + ax + (a+b)$ ⇐ b1

- $\boxed{x^{-1}}$: $GF((2^2)^2)$ 상의 역원.

$(ax+b)^{-1} = a(a^2\phi + (a+b)b)^{-1}x + (a+b)(a^2\phi + (a+b)b)^{-1}$ 꼴이다.



$\boxed{\times}$: $GF(2^2)$의 유한체 곱셈 연산기

$I_1, I_2 \to \boxed{\times} \to O \Rightarrow$

<output>

$I_1 \backslash I_2$	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

$I \to \boxed{x^{-1}} \to O \Rightarrow$

<output>

I	
00	00
01	01
10	11
11	10

$I \to \boxed{x^2} \to \boxed{\times\phi} \to O \Rightarrow$

$(\phi = 10)$

<output>

I	
00	00
01	10
10	01
11	11

$\therefore$ $GF((2^2)^2)$ 상의 역원

→

Input	Inversion
0000	0000
0001	0001
0010	0011
0011	0010
0100	1111
0101	1100
0110	1001
0111	1011
1000	1010
1001	0110
1010	1000
1011	0111
1100	0101
1101	1110
1110	1101
1111	0100

⇒ LUT로 구현.

· $GF((2^2)^2)$ 곱셈기.

$(AY+B)(CY+D)$ (A,B,C,D는 2bit)

$= ACY^2 + BCY + ADY + BD$

$= AC(Y+\phi) + BCY + ADY + BD$

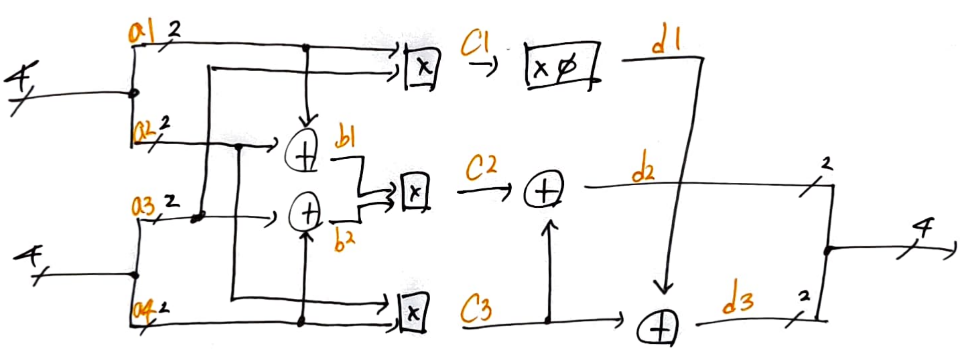
$= Y(AC+BC+AD) + AC\phi + BD$ → 4개의 곱셈기 필요

$= Y(AC+BC+AD+2BD) + AC\phi + BD$

추가 ($\because 2BD=0$)

축소

$= Y((A+B)(C+D)+BD) + AC\phi + BD$ → 3개의 곱셈기 필요



$\boxed{x}$: $GF(2^2)$ 곱셈기.

→ $\boxed{x\phi}$ →

C1에서 $(ax+b)$ 꼴로 들어온다고 하면,

$(ax+b)\times\phi$

$=(ax+b)\times x$

$=ax^2+bx$

$=a(x+1)+bx$

$=(a+b)x+a$. → d1

· GF(2^2) 곱셈기.

$(ax+b)(cx+d)$ (a, b, c, d는 1bit)

$= acx^2 + bcx + adx + bd$

$= ac(x+1) + bcx + adx + bd$

$= x(ac+bc+ad) + ac + bd$

$= x(ac+bc+ad+2bd) + ac + bd$

$= ((a+b)(c+d)+bd)x + ac + bd$