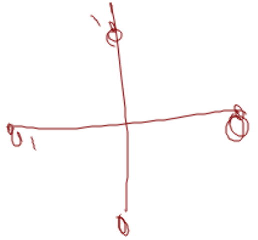
$$\alpha \oplus \beta = \left(\frac{\alpha_1 \beta_2 + \alpha_2 \beta_1}{1 + d\,\alpha_1 \alpha_2 \beta_1 \beta_2},\ \frac{\alpha_2 \beta_2 - a\,\alpha_1 \beta_1}{1 - d\,\alpha_1 \alpha_2 \beta_1 \beta_2} \right)$$

Pokud ∀ body grupy na křivce, tak mám pro všechny výpočty jedinou formuli. ← uzavřená formule
closed
universal

z toho plyne rezistence odolnost na side channel attacks (útoky postranními kanály)



$$(1,0) \oplus (b_1, b_2) = (b_2, -b_1)$$

$$(1,0) \oplus (1,0) = (0,-1) \qquad [4](1,0) = (0,1)$$

$$(1,0) \oplus (0,-1) = (-1,0) \qquad [2](1,0) = (0,-1)$$

$$(1,0) \oplus (-1,0) = (0,1)$$

Na Edwardsově křivce existují body řádu 4

Platí to i naopak.

Každá WK $y^2 = f(x)$ s bodem řádu 4 je biracionálně ekvivalentní nějaké Edw. křivce.

Pokud WK $y^2=f(x)$ obsahuje bod P řádu 4, pak $[2]P$ je bod řádu 2 (involuce). Involuce WK známe. To jsou všechny body $(\xi, 0)$, kde $f(\xi)=0$. Ať tedy $(\xi, 0)$ lze dostat jako $[2]P$. Zvolme transformaci, $f(x) = \tilde{f}(x-\xi)$. Pak $(0,0)$ je involuce na WK $y^2=\tilde{f}(x)$, která je zdvojením nějakého bodu řádu 4, jinými slovy. Stačí uvažovat birac. ekv. pro WK

$$y^2 = x^3 + a_2 x^2 + a_4 x,$$ kde $(0,0) = [2](\alpha, \beta)$

Připomeňme vzorec pro [2]

$$(\alpha,\beta) \longmapsto (-2\alpha+\lambda^2-a_2, \dots) = (\gamma,\delta)$$

$$\lambda = \frac{3\alpha^2+2a_2\alpha+a_4}{2\beta}$$

Pokud $\gamma=0$ tak $\delta=0$ neboť $y^2=x^3+a_2x^2+a_4x$

0 je jednoduchý kořen

2. Co musí a_4, a_6 splňovat, aby $\exists\,(\alpha,\beta)$ na křivce, že $-2\alpha+\lambda^2-a_2=0$

$$(2\beta)^2 = 4\beta^2 = 4(\alpha^3+a_2\alpha^2+a_4\alpha)$$

$$(\alpha^3+a_2\alpha^2+a_4\alpha)(\alpha+a_2) = 2\alpha^4+3a_2\alpha^3+(2a_4+a_2^2)\alpha^2+a_2a_4\alpha$$

$$0=\gamma\lambda^2 = -8\alpha\beta^2+(3\alpha^2+2a_2\alpha+a_4)^2-a_2 4\beta^2 =$$

$$= 9\alpha^4+12a_2\alpha^3+(6a_4+4a_2^2)\alpha^2+4a_2a_4\alpha+a_4^2$$

$$-8\alpha^4-12a_2\alpha^3-(8a_4+4a_2^2)\alpha^2-4a_2a_4\alpha = \alpha^4-2a_4\alpha^2+a_4^2$$

$$=(\alpha^2-a_4)^2$$

a_4 musí být druhou mocninou

$$\alpha^3 + a_2\alpha^2 + a_4\alpha = \alpha^2(2\alpha + a_2) = \beta^2$$

[2] $(\alpha,\beta) = (0,0)$ $\quad \alpha^2$

$2\alpha + a_2$ je také čtverec

$(\xi, 0)$

je dvojnásobný nejmenší bod na křivce

$y^2 = f(x)$

Nyní $\exists \lambda$, že $\lambda = \alpha$

$a_4 = \lambda^2$

$a_2 + 2\lambda$ také čtverec

Transformace MK na WK

Hledáme A, B, že $B = \lambda$

$a_2 = AB$

$a_4 = B^2$

$a_2 + 2\lambda \quad \lambda = B$

$(AB + 2B)$ je čtverec

$a = \frac{A+2}{B}$

$A = \frac{a_2}{B}$

y^2

$ax^2 + y^2 = 1 + dx^2y^2$

$(\gamma x)^2 + y^2 = 1 + d\gamma^{-2}(\gamma x)^2 y^2$

JE K-ekvivalentní Edw. křivce

MK $\rightarrow$ Edw. K

a čtverce

$a = \frac{A+2}{B} = \frac{\frac{a_2}{\lambda} + 2}{B} = \frac{a_2 + 2\lambda}{\lambda^2}$

Twisted ← zkroucený / překroutit / přepólovat

skrut

předkloněný

Edwards curves

čtverec → nečtverec

$$1 + dx^2y^2 = ax^2 + y^2$$

← a čtverec · ekvivalentní Edw. křivce

← a nečtverec

zobecněný Edw. křivka