JubJub 曲线

谢文进

2024 年 1 月 7 日

目录

1 JubJub 曲线

1.1 Baby JubJub vs. JubJub

表 1: Baby JubJub vs. JubJub

	Baby JubJub	JubJub
Montgomery curve	$y^2 = x^3 + 168698x^2 + x$	$y^2 = x^3 + 40962x^2 + x$
Twisted Edwards curve	$168700x^2 + y^2 = 1 + 168696x^2y^2$	$40964x^2 + y^2 = 1 + 40960x^2y^2$
After scaling	$-x^2 + y^2 = 1 + (-168696/168700)x^2y^2$	$-x^2 + y^2 = 1 + (-10240/10241)x^2y^2$

1.2 Montgomery curve

BLS12381 的阶:

$p = 52435875175126190479447740508185965837690552500527637822603658699938581184513$

JubJub 曲线: $y^2 = x^3 + 40962x^2 + x$

$n = h \times l$, 其中 $h = 8$

$$n = 52435875175126190479447740508185965837647370126978538250922873299137466033592$$

$$l = 6554484396890773809930967563523245729705921265872317281365359162392183254199$$

生成元: $G_0^M = (x_0^M, y_0^M)$

$$x_0^M = 10,$$

$$y_0^M = 48640165556916281326586888156651996935661899782624607295706115105756532634 43$$

base point $G_1^M = (x_1^M, y_1^M)$

$$x_1^M = 18662558417428907826588413824421338451096304318249267443782476967941530951665,$$

$$y_1^M = 10829583678449754674258847202008243338777477689250089851084221267577753407818$$

1.3 Twisted Edwards curve

曲线方程：$40964x^2 + y^2 = 1 + 40960x^2y^2$
生成元：$G_0 = (x_0, y_0)$

$$x_0 = 50210964013865202807697778192253911217867412634541528443086291916476367487291,$$

$$y_0 = 95337954863865800871723164560338119704891913637322977859279379454433783971 85$$

base point $G_1 = (x_1, y_1)$

$$x_1 = 25048732578063176751608348748134148938511950496662102134944680124345451629928,$$

$$y_1 = 37193546711722353718211339597021920218737743307281823076963067517006020382455$$

1.4 scale

Theorem 6. Consider a twisted Edwards curve defined over Fp given by equation $ax^2 + y^2 = 1 + dx^2y^2$. If $-a$ is a square in $\mathbb{F}_p$, then the map $(x, y) \to (x/\sqrt{-a}, y)$ defines the curve $-x^2 + y^2 = 1 + (-d/a)x^2y^2$. We denote by $f = \sqrt{-a}$ the scaling factor.

因此曲线 $40964x^2 + y^2 = 1 + 40960x^2y^2$ 等价于曲线 $-x^2 + y^2 = 1 + (-10240/10241)x^2y^2$. scaling factor 为 $f = \sqrt{-40964}$.