Let us consider for a moment both the curves above in the Standard Projective coordinates, because the implementation attached in the paper utilizes that coordinate system

$$(6)\ \begin{cases} E: Y^2Z = X^3 + aXZ^2 + bZ^3 \\ E^d: Y^2Z = X^3 + ad^2XZ^2 + bd^3Z^3 \end{cases}$$

Now define the set:

$$S = \{\underbrace{(0:1:0)}_{=\Theta}\} \cup \{(x:y:1) \in E(K\sqrt{d}) \text{ with } x \in K \text{ but } y \in K(\sqrt{d})\}$$

That is $a, b, x \in K$, but we allow y to belong to $K(\sqrt{d})$.

We can split S into subsets:

$S = \{\Theta\} \cup S^0 \cup S^1 \cup S^2$ where

$S^0 = \{(x:0:1) \in E(K(\sqrt{d}))$, with $x \in K\}$ – – points of order 2

$S^1 = \{(x:y:1) \in E(K(\sqrt{d}))$, with $x \in K$, $y \in K^*\}$,

$S^2 = \{(x:y:1) \in E(K(\sqrt{d}))$, with $x \in K$, $\underline{y \in K(\sqrt{d}) \setminus K}\}$

Note, however, that y __is not__ of the form $\alpha + \beta\sqrt{d}$ for $\alpha \neq 0$, otherwise $y^2 = (\alpha + \beta\sqrt{d})^2 = \alpha^2 + \beta^2 d + 2\alpha\beta\sqrt{d} \notin K$ for $\alpha \neq 0$ and $\beta \neq 0$

but $y^2 = \underbrace{x^3 + ax + b}_{\in K}$

Hence in S^2 we have $y = \beta \cdot \sqrt{d}$ for $\beta \in K^*$

We remember from (3) and (4) that

$\left(\frac{x}{d}, \frac{y}{d\sqrt{d}}\right)$ satisfies equation (1) of E

iff (x, y) satisfies equation (3) of the first E^d.

Note that

$$\left(\frac{x}{d}, \frac{y}{d\sqrt{d}}\right) = \left(\frac{x}{d}, \frac{y\sqrt{d}}{d^2}\right).$$

See that for each point $(x', y') \in S^2$ we easily find $x \in K$, $y \in K^*$ such that $(x', y') = (x \cdot d^{-1}, y \cdot d^2 \sqrt{d})$.

Consequently, each point $(x', y') \in S^2$ corresponds to some point $(x, y) \in E^d$, where $x \in K$, $y \in K^*$. The reverse is also true:

each $(x, y) \in E^d$, where $x \in K$, $y \in K^*$, corresponds to $\underbrace{(x d^{-1}, y \cdot d^{-2} \cdot \sqrt{d})}_{\in S^2}$ on E

If we define S_d for E^d as we defined S for E then it is easy to show that S^0 corresponds to S^0_d, S^2 corresponds to S^1_d and S^1 corresponds S^2_d ("corresponds" means that there is 1-to-1 mapping). On the other hand

$S^0 \cup S^2$ may be described by the "curve" $\underline{d\hat{y}^2 = x^3 + ax + b}$, where both $x, \hat{y}$ are in K. $\updownarrow$

$$(\hat{y}\sqrt{d})^2 = x^3 + ax + b$$

So regarding $S^0 \cup S^2$, because it corresponds to $S^0_d \cup S^1_d$, there is 1-to-1 correspondence of the "curve"

$$d y^2 = x^3 + ax + b$$ and the curve $$y^2 = x^3 + ad^2x + bd^3.$$

Consequently, for $S^0 \cup S^2$ we can equivalently use each of the two equations of the twist:

$$d y^2 = x^3 + ax + b$$

$$y^2 = x^3 + ad^2x + bd^3$$

or the corresponding projective form.

Now assume that $K = \mathbb{F}_p$. Let t be the number of points of order 2. Note that for each x such that $x^3 + ax + b \neq 0$ there are two different $y \neq 0$ such that

$(x : y : 1) \in S$.

Of course $\mathcal{O} \in S$ thus

$|S| = 1 + \underbrace{2p}_{} - t$

x yielding 0 on the RHS of EC equation are counted twice in $2 \cdot p$

On the other hand, from the Hasse theorem, the set $\{\mathcal{O}\} \cup S^0 \cup S^1$ has $\boxed{p+1-c}$ distinct points for c such that $|c| \leq 2\sqrt{p}$

for $x^3 + ax + b = s$ the s QN p

$s \cdot d$

odd powers of generator so the result is an even power

so there is $y \in K^*$

$y^2 = s \cdot d$

$$\left(\frac{y}{\sqrt{d}}\right)^2 = s$$

$$\left(\frac{y\sqrt{d}}{d}\right)^2 = s$$

$$\left(x, \frac{y\sqrt{d}}{d}\right) \in S^2$$

$$\left(x, \frac{-y\sqrt{d}}{d}\right) \in S^2$$

$$p+1-2\sqrt{p} \leq \underbrace{\#E(\mathbb{F}_p)}_{\uparrow} \leq p+1+2\sqrt{p}$$

$$p+1-c \qquad |c| \leq 2\sqrt{p}$$

Consequently, cardinality of S^2 equals

$$|S| - |E(\mathbb{F}_p)| = 2p+1-t-(p+1-c) =$$

$$= p+c-t$$

and cardinality of $\{O\} \cup S^0 \cup S^2$ — the elements of E^d

equals:

$$\overline{p+c-\cancel{t}} + 1 + \cancel{t} = \boxed{p+1+c}.$$

That is, if we know the cardinality of E (equal to $p+1-c$) then we immediately learn the cardinality of E^d (equal to $p+1+c$).

Note that if $p+1-c$ is a prime number then not necessarily $p+1+c$ is a prime as well...

To discuss the fault injection attack we need to introduce:

- Montgomery Ladder
- optimization of the EC arithmetic by:
  - removing y-coordinate from the computations
  - calculating point addition and point doubling in a single procedure.

Let us start with the Montgomery Ladder: