Fault Attacks on Elliptic Curve with Montgomery ladder implementation

In this chapter we shall learn about some fault injection attack on a point multiplication procedure that does not use y-coordinate. The paper from the title has been published in 2008.

The attack is successful if the so called twist of an elliptic curve attacked has smooth order.

no large prime factors ?

To understand the attack we shall learn a few mathematical tools:

- definition of an isomorphism between elliptic curves,
- definition of the twist of an elliptic curve
- different formulas for the twist,
- the right relation between the order of the curve and the order of the twist.

We need to start from the definition of an elliptic curve.

The equation (1) known from the first lecture:

(1) $y^2 = x^3 + ax + b$

defining an elliptic curve for fields of characteristic $\neq 2, 3$ is a

short form of the equation:

$$(2)\quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$a_i \in K$$

The equation above is known as the Weierstrass form of an elliptic curve E, and is valid for any characteristic. The characteristic-specific forms are derived from (2).

Definition:

The elliptic curves defined over a field K:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$E': y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

are isomorphic over K if E' can be obtained from E by a change of variables of the form:

$$\psi: \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} u^2x + r \\ u^3y + u^2sx + t \end{pmatrix} =$$

$$= \begin{pmatrix} u^2 & 0 \\ u^2s & u^3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} r \\ t \end{pmatrix}$$

where $u \in K^*$, $r, s, t \in K$; and dividing the resulting equation by u^6.

The corresponding transformation ψ is refered to as an admissible change of variables.

The curves defined by projective Weierstrass equations:

$$E: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

$$E': Y^2Z + a_1'XYZ + a_3'YZ^2 = X^3 + a_2'X^2Z + a_4'XZ^2 + a_6Z^3$$

are isomorphic if E' can be obtained from E by a change of variables of the form:

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \longmapsto \begin{pmatrix} u^2X + rZ \\ u^3Y + u^2sX + tZ \\ Z \end{pmatrix}$$

for $u \in K^*$, $r, s, t \in K$; and dividing the resulting equation by u^6.

Definition:

Let $E: y^2 = x^3 + ax + b$. The (quadratic) twist of E by a quadratic non-residue $d \in K^*$ is the curve E^d given by equation:

↑ the term "quadratic" is often skipped

$$(3) \quad y^2 = x^3 + ad^2x + bd^3$$

Equation (3) is satisfied iff

$$(4) \quad \frac{y^2}{d^3} = \frac{x^3}{d^3} + a\frac{x}{d} + b$$

is satisfied. So from (4) and (3) we have that the point $\left(\frac{x}{d}, \frac{y}{d\sqrt{d}}\right)$ satisfies equation (1) iff (x, y) satisfies equation (3).

Setting $u = (\sqrt{d})^{-1}$, $r = s = t = 0$ we get the isomorphism from E to E^d;

Indeed:

$$\psi: \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \frac{x}{d} \\ \frac{y}{d\sqrt{d}} \end{pmatrix}$$

$$\left(\left(\frac{y}{d\sqrt{d}}\right)^2 = \frac{x^3}{d^3} + a\frac{x}{d} + b\right) \cdot \left(u^6\right)^{-1}$$

$$u^6 = \left((\sqrt{d})^{-1}\right)^6$$

$$\text{so } \left(u^6\right)^{-1} = d^3$$

Hence the resulting curve is:

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

Note, however, that since d is not a quadratic residue in K, than $\sqrt{d} \notin K$

But $\sqrt{d} \in K(\sqrt{d}) = \{\alpha + \beta\sqrt{d},\ \alpha, \beta \in K\}$

note that higher powers of $\sqrt{d}$ like e.g. $(\sqrt{d})^k$ collapse to $(\sqrt{d})^{k \bmod 2} \cdot (\sqrt{d})^{2\cdot\lfloor k/2 \rfloor} = (\sqrt{d})^{k \bmod 2} \cdot (d)^{\lfloor k/2 \rfloor}$

In case of a finite field $K = \mathbb{F}_p$ we get that $\mathbb{F}_p(\sqrt{d})$ has p^2 elements (α, β can be chosen independently) and $\mathbb{F}_p(\sqrt{d})$ can be denoted by $\mathbb{F}_{p^2}$

So we see that the curves

$$(5) \begin{cases} E: & y^2 = x^3 + ax + b \\ E^d: & y^2 = x^3 + ad^2x + bd^3 \end{cases}$$

are isomorphic over $K(\sqrt{d})$ but not over K.

$\mathbb{F}_p[X]/(f)$
$f(X) = X^2 - d$ $a_0 + a_1 X$

exactly the same situation like
$i = \sqrt{-1} \notin \mathbb{R}$
but $i \in \mathbb{R}(i) = \mathbb{C}$