Add a When $M_{i+1} \to M_i$ is an addition then, for

$$M_i = (X_i, Y_i, Z_i)$$

$$M_{i+1} = (X_{i+1}, Y_{i+1}, Z_{i+1})$$

$$G = (X_G, Y_G, Z_G) = (x_G, y_G, 1)$$

↑ affine coordinates of G

$$Z_i = Z_G \cdot Z_{i+1}(X_{i+1} Z_G^2 - X_G Z_{i+1}^2) =$$

$$= 1 \cdot Z_{i+1}(X_{i+1} - x_G \cdot Z_{i+1}^2) =$$

↑ affine $x_{i+1} = \frac{X_{i+1}}{Z_{i+1}^2}$

$$= Z_{i+1}^3 (\underbrace{x_{i+1}}_{\text{we are able to calculate this as a correct affine coordinate of } P-G} - X_G)$$

$$\underbrace{Z_i \cdot (x_{i+1} - X_G)^{-1}}_{(*)} = Z_{i+1}^3$$

For some values (*) of $p \equiv 1 \pmod 3$, where p determines the field arithmetic, there is no such Z_{i+1} whose third power yields left hand side of the above equation.

On the other hand, if the cubic root exists, then usually there are three such roots:

Let q be a prime number. We shall show that if q divides $|\mathbb{F}_p^*|$ (the cardinality of the multiplicative group $\mathbb{F}_p^*$) then a fraction $\frac{1}{q}$ of elements of $\mathbb{F}_p^*$ is a q-th power of some other elements. That is, for such a fraction of elements there exists a q-th root of a given element.

Moreover, if for a given element its q-th root exists then there are q such roots.

Let

$$|\mathbb{F}_p^*| = p-1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

be the prime factorization of the group order ($p_i < p_j$, $i<j$, p_i, $i=1,2,\ldots,k$ are prime numbers).

Since p_i are primes then $q = p_j$ for some j.

Let g be a generator of $\mathbb{F}_p^*$. Luckily, for any finite field there exists a generator of its multiplicative group.

So for any $b \in \mathbb{F}_p^*$ there is some x such that

$$b = g^x$$

in $\mathbb{F}_p^*$.

Since $\operatorname{ord} g = p-1$ we have implicit modular arithmetic in the exponent of g.

The modulus equals $p-1$.

From the Chinese Reminder Theorem we know that there is 1-to-1 correspondence between elements x modulo $p-1$ an the sequences of congruences:

$$\begin{cases} x \equiv x_1 \pmod{p_1^{\alpha_1}} \\ \vdots \\ x \equiv x_k \pmod{p_k^{\alpha_k}} \end{cases}$$

where $x_i \in \{0, \ldots, p_i^{\alpha_i} - 1\}$

Moreover,

$$x \equiv \sum_{i=1}^{k} x_i M_i N_i \pmod{\underbrace{\prod_{i=1}^{k} p_i^{\alpha_i}}_{p-1}},$$

where $M_i = (p-1)/p_i^{\alpha_i}$

$$N_i \cdot M_i \equiv 1 \pmod{p_i^{\alpha_i}}$$

Hence, if a is a q-th power of some b, then:

$$a = b^q \equiv b^{p_j} = g^{x p_j} = g^y \qquad (p_j = q)$$

and:

$$\begin{cases} y \equiv y_1 \pmod{p_1^{\alpha_1}} \\ y \equiv y_2 \pmod{p_2^{\alpha_2}} \\ \cdots\cdots \\ y \equiv y_j \pmod{p_j^{\alpha_j}} \\ \cdots\cdots \\ y \equiv y_k \pmod{p_k^{\alpha_k}} \end{cases}$$

and $y_i \equiv x_i p_j \pmod{p_i^{\alpha_i}} \quad i = 1, 2, \ldots, k$

And for $i \neq j$ p_j is invertible modulo $p_i^{\alpha_i}$ hence modulo such $p_i^{\alpha_i}$ multiplication (in the exponent) by p_j is a bijection.

For $i = j$ the situation is different.

Write x_j in the positional system in base p_j:

$$x_j = (x_{j,\alpha_j - 1}\ x_{j,\alpha_j - 2} \cdots x_{j,0})_{p_j}$$

then

$$x_j \cdot p_j = (x_{j,\alpha_j - 2}\ x_{j,\alpha_j - 3} \cdots x_{j,0}\ 0)_{p_j}$$

That is y_j has the least significant digit in base p_j equal to 0.

So there is a fraction of $\frac{1}{q}$ elements of $\mathbb{F}_p^*$ satisfying this condition

so $a^{\frac{p-1}{p_j}} \equiv 1 \pmod{p}$

Moreover, such y_j corresponds to q element x_j such that:

$$y_j = x_j \cdot p_j \pmod{p_j^{\alpha_j}}$$

because the digit $x_{j,\alpha_j - 1}$ disappeared in y_j and there are q possibilities for this digit. (y_i corresponds to single x_i for $i \neq j$ because of invertibility of p_i modulo $p_i^{\alpha_i}$).

If $a \equiv 0 \pmod{p}$ then of course q-th root from a is 0, so in this case we have 1-to-1 mapping.

Thus, if

$$z_i (x_{i+1} - x_G)^{-1}$$

is not a third power of some element in $\mathbb{F}_p^*$ then the step $M_{i+1} \to M_i$ could not be an addition.

If we have not eliminated "the addition" possibility we have to find all candidate values z_{i+1} and for each one reconstruct x_{i+1}, y_{i+1} from the property

$$M_{i+1} = M_i - G = M_i + (-G)$$

Hence we have at most three candidates for

$$M_{i+1} = (x_{i+1}, y_{i+1}, z_{i+1})$$

and then $M_{i+2} \to M_{i+1}$ must be a doubling.

Ad b) When a ~~stop~~ $M_{i+1} \to M_i$

is a doubling then, from the point-doubling formulas:

$$Z_i = 2\, Y_{i+1}\, Z_{i+1} = 2\, y_{i+1} Z_{i+1}^4$$

↑ affine coordinate

so $$\frac{Z_i}{2 y_{i+1}} = Z_{i+1}^4$$

Note that affine coordinates (x_{i+1}, y_{i+1}) can be reconstructed from M_i utilizing the dependencies

$$M_i = 2\, M_{i+1} \,/\, 2^{-1} \pmod{\text{ord } G}$$

(it should be a prime number) $= L$

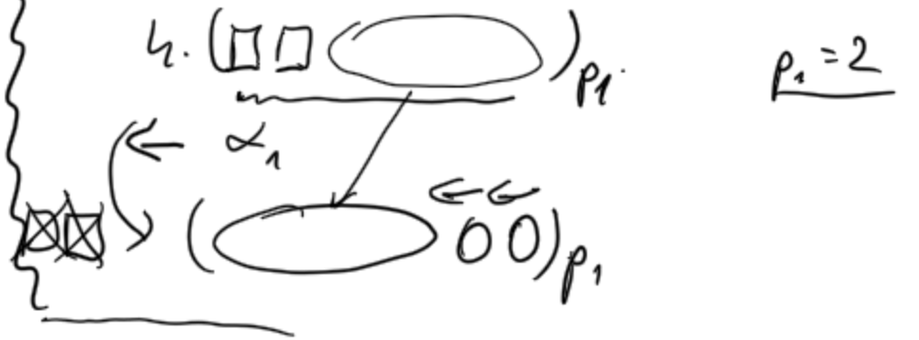
$$L \cdot M_i = M_{i+1}$$

for scalar $L = 2^{-1} \pmod{\text{ord } G}$

If $p \equiv 1 \pmod 4$ then a quarter of

$2^2 \mid p-1$

$p_1 = 2 \qquad \alpha_1 \geq 2$



$p_1 = 2$

random elements

$$\frac{Z_i}{2 y_{i+1}}$$

is a 4-th power of some element, and if it is the case then there are four roots Z_{i+1}.

If $p \equiv 3 \pmod 4$ then a half of inputs (if they are non-zero)

$$\frac{z_i}{2y_{i+1}}$$

is a fourth power of some other element.

$p \equiv 3 \pmod 4$ $\quad p = 4k+3$

$p-1 = 4k+2 = 2(2k+1)$

$p-1 = 2^1 \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$

$p_i \neq 2$

$\alpha_1 = 1$

$(\square)_2$ ← 1 digit

← 2 power

$\square(.0)_2$

← 2 power

$(g^x)^4 =$ ← 4 possible

~~So if $\frac{z_i}{2y_{i+1}}$ is not a~~

and if it is the case there are two (4th) roots of such an element.

So if $\frac{z_i}{2y_{i+1}}$ is not a fourth power of some element of $\mathbb{F}_p$ then the step $M_{i+1} \to M_i$ could not be a doubling.

If we have not eliminated "the doubling" possibility we have to find all the candidate values $2y_{i+1}$ and for each one we reconstruct x_{i+1}, y_{i+1} from

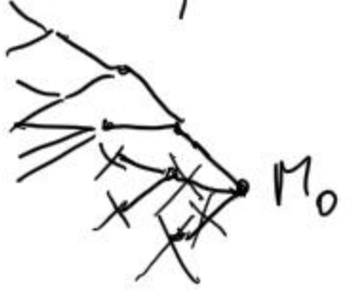
$$L \cdot M_i = M_{i+1}.$$

Finally, if we have Jacobian coordinate representation of $P = k \cdot G$ we assign $M_0 = P$ and we try to reconstruct the trailing bits of k by back-tracking:

$$M_2 \xrightarrow{\text{doub}} M_1 \xrightarrow{\text{add}} M_0$$ when we test for $k_0 = 1$

$$M_1 \xrightarrow{\text{doub}} M_0$$ when we test for $k_0 = 0$

and we continue with bits k_1, k_2, etc. if the number of emerging sequences S_i is low



The paper "Projective coordinates leak" indicate that

$$Pr[k_0 \text{ determined correctly}] = 0.96$$

for $p \equiv 1 \pmod{12}$

For $p \equiv 5 \vee 7 \vee 11$ the results are weaker.

Moreover, similar analysis for the Standard Projective Coordinates is provided in the paper.

In the more recent paper "From A to Z: Projective coordinates leakage in the wild" an attack to the libcrypt library is presented. The attack utilizes the result above and the side channel information.