Projective coordinates leak

Let us assume that:

1) The result of scalar multiplication:

$$P = k \cdot G$$

is available to the adversary in projective coordinates. E.g., by a side-channel attack the adversary is able to find

$$(X, Y, Z),$$

which is an internal representation of P in projective coordinates.

2) For simplicity assume that $k \cdot G$ is calculated with the double-and-add algorithm.

However, the attack works for other methods as well.

The double-and-add method:

Let $(k_\ell k_{\ell-1} \dots k_0)_2$ be the binary representation of k, and $k_\ell = 1$.

The result $P = k \cdot G$ is calculated as follows:

```
P := G
for (i := l-1; i >= 0; i--) {
    P := 2·P
    if (k_i == 1)  P := P + G
}
return P.
```

3) Let us fix our attention on the Jacobian coordinates. The standard projective coordinates

shall be summarized later.

The curve $E_{a,b}$ is defined over $\mathbb{F}_p$, where p is prime.

The aim of the attack is to find the last t bits of k.

Each candidate sequence of bits

$$\underbrace{k_{t-1}\, k_{t-2} \ldots k_1\, k_0}_{t \text{ bits}}$$

corresponds to a sequence of operations: point doubling and point addition.

Let s_j be a sequence of intermediate points determined by the operations:

$$s_j = \{ M_u^{(j)} \to M_{u-1}^{(j)} \to \ldots \to M_0^{(j)} \}$$

where $M_0^{(j)} = P$.

The arrows above denote additions of G to P or doublings.

We will try to reverse the sequence s_j, that is to move from M_0 to M_1, further to M_2, etc., until t-trailing bits of k are revealed.

Sometimes we are successful.

For each step:

$$M_{i+1} \to M_i$$

we have two possibilities at most:

a) $M_{i+1} \to M_i$ is an addition

b) $M_{i+1} \to M_i$ is a doubling.

but if $M_{i+1} \to M_i$ is an addition then (double and add method) $M_{i+2} \to M_{i+1}$ must be a point doubling.

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

$$= Z_{i+1}^3 (\underbrace{x_{i+1}} - x_G)$$

we are able to calculate this as a correct affine coordinate of P−G.

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

For some values (*)