“Nice” EC params summary

Quick reminder about EC

Elliptic curve (in Weierstrass form) is a curve which is defined by:

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

In order to do some operations on it, we should define an Abelian group on points on this curve, and to do that we would need to add an *ideal*, which is usually denoted ∞.

Then, operations on the curve can be defined for any two points $P = (x_P, y_P), Q = (x_Q, y_Q)$ as follows:

$$\begin{aligned}
\infty + P &= P \\
\infty + \infty &= \infty \\
P + Q &= R \\
\lambda &= \frac{y_Q - y_P}{x_Q - x_P} \\
x_R &= \lambda^2 - x_P - x_Q \\
y_R &= \lambda(x_P - x_R) - y_P
\end{aligned}$$

Multiplication by a scalar can be done with stacked addition:

$$nP = \underbrace{P + P + ... + P}_{n \text{ times}}$$

Now we're ready to do crypto! In order to operate on integers, let's take any finite field $F(p)$, and then use the coordinates from that field.

This is an asymmetric scheme, so let's define the public and private keys. Before that, though, we would need to agree on some common parameters - the curve itself is defined by a and b from the equation, the field would be defined by p for prime fields, or m and f for binary fields, and we need to take some cyclic subgroup of the whole group of points, so G would be the generator of such group.

So, EC params (for prime fields) are: (p, a, b, G). Finally, let's say that a private key would be any element of the base field - k, and the public key would be a point on the curve - kG.

ECDLP here would be to derive k from kG, and that is hard, because we use a finite field.

The problem

The problem of designing a “nice” curve would be to provide such elliptic curve parameters, that they look OK to the user that would generate the key, while allowing us to do ECDLP or decryption (or signature) without knowing their private key (usually knowing only their public key).

One way to do that would be to create a degenerate case, e.g. some set of parameters that would make that curve translate into something more simple, such as a straight line, or a polynomial in terms of first powers of x and y.