El protocolo de firma digital para curvas elípticas se basa en el protocolo de firma de ElGamal. Dada una curva elíptica definida sobre un cuerpo finito F de q elementos, donde G el punto base de la curva elíptica (generador), con orden es n y su cofactor es c. La clave pública de Alice (firmante) es $(G, Q = d \cdot G)$ y la privada es d.

Firma digital ECDSA

Algoritmo 4 Firma ECDSA

Entrada: La clave pública y privada de Alice Q y d.
Salida: Mensaje M y la firma (r, f)

1: Alice calcula el resumen (hash) del mensaje a firmar: $h(M) = m$.

2: Alice genera la clave de sesión: elige al azar un número secreto, k, $0 < k < q - 1$ tal que $\text{mcd}(k, q - 1) = 1$.

3: Alice calcula los siguientes dos valores:

$$kG = (x, y),$$
$$r \equiv x \bmod q.$$

Si $r = 0$, Alice elige otro valor para k.

4: Luego Alice calcula,

$$f = k^{-1}(m + x \cdot r) \bmod q.$$

5: **return** $M, (r, f)$