§ 4.3. Signature avec CE. (Courbes elliptiques)

CE. : 160 – 256 bits Contre. 1024 – 3072 bits.
RSA et DL.

La signature avec CE est analogue à DSA, sur $\mathbb{Z}_p$.

Génération de clés

1. Soit E une courbe elliptique avec
   - p module
   - a, b coefficients
   - pt A engendrant le groupe cyclique d'ordre premier q.
2. Choisir aléatoirement $0 < d < q$
3. $B = dA$

Clés : $k_{pub} = (p, a, b, q, A, B)$

$k_{pr} = (d)$.

Signature CE.

1. Choisir alea. k_E, $0 < k_E < q$.
2. $R = k_E \cdot A$.
3. $r = x_R$ (coordonnée x de R).
4. Calculer $s = (h(x) + d \cdot r) \cdot k_E^{-1} \bmod q$

h : fonction de hachage