Proposition Le schéma DSA de signature ci-dessus est correct.

preuve • D'abord penser que faut-il prouver, i.e. DSA est correcte ?

Celà revient à montrer que $Sig_{Pr.}(x) = (r, s)$ vérifie la condition $v \equiv r \pmod q$.

$$s \equiv (SHA(x) + d \cdot r) \cdot k_E^{-1} \pmod q.$$

$$\Rightarrow \quad k_E = s^{-1} SHA(x) + d s^{-1} r \pmod q.$$

$$= u_1 + d u_2 \pmod q$$

$$\Rightarrow \quad \alpha^{k_E} \pmod p = \alpha^{u_1 + d u_2} \pmod p$$

$$= \alpha^{u_1} \cdot \beta^{u_2} \pmod p$$

on réduit $\pmod q$:

$$(\alpha^{k_E} \bmod p) \bmod q = ((\alpha^{u_1} \cdot \beta^{u_2}) \bmod p) \bmod q.$$

Comme $r = (\alpha^{k_E} \bmod p) \bmod q$ et $v = (\alpha^{u_1} \beta^{u_2} \bmod p) \bmod q$

$$\Rightarrow \quad r \equiv v \pmod q. \quad \square$$

Rq • la génération de clé est l'étape qui demande plus de calcul (engendrer p, q ; utiliser un générateur de nbrs premiers).

Attaques non génériques pour PLD. (2 fois).