Prop. Le schéma ci-dessus est correct.

Preuve. on a :

$$\beta^r \cdot r^s \equiv (\alpha^d)^r \cdot (\alpha^{k_E})^s \pmod p.$$
$$\equiv \alpha^{dr + k_E \cdot s} \pmod p$$

La signature est valide si $\beta^r \cdot r^s \equiv \alpha^x \pmod p$! c.à.d si

$$\alpha^x \equiv \alpha^{dr + k_E \cdot s} \pmod p \quad (1).$$

D'après le théorème de Fermat, la relation (1) est vraie si

$$x \equiv dr + k_E \cdot s \pmod{p-1}.$$

càd si $s \equiv (x - dr) \cdot k_E^{-1} \pmod{p-1}$.

Ce qui est vrai par la construction 2. du protocole génération de la signature ci-dessus ☐.

- **Calcul et sécurité de ELGAMAL.**

→ La phase SETUP est identique à celle du cryptage (cf §. ELGAMAL, chap 3). La même difficulté revient à calculer le LD que précédemment.
On utilise des calculs rapides ↯ (M and S), exponentiation modulaire, Euclide Etendu. $p \geq 1024$.

→ **Attaque lorsque k_E est ré-utilisée :**

Supp que x_1 et x_2 ont même clé éphémère k_E. ⇒ $r_1 = r_2 = \alpha^{k_E} \cdot$ et

$$\begin{cases} s_1 \equiv (x_1 - d) k_E^{-1} \pmod{p-1} \\ s_2 \equiv (x_2 - d) \cdot k_E^{-1} \pmod{p-1}. \end{cases}$$

avec deux inconnues d (clé privée) et k_E.