Soient

$$(s_i)_{i=1,\ldots,n} \text{ de privé} \quad \text{et} \quad \forall i \in \{1,\ldots,n\},\ v_i = s_i \times G$$

$$(t_i)_{i=1,\ldots,n} \text{ de public}$$

Soit f qui prend $(a_1, a_2, \ldots, a_{n-1}, t_1, t_2, \ldots, t_n) \in \mathbb{R}^n \times \mathbb{R}^n$ (on note $P = 1 + \sum_{k=1}^{n-1} a_k X^k$, polynôme de degré $n-1$ et non nul donc $n-1$ racines), et qui renvoie

$$(P(1)S_1 - t_1 G, \ldots, P(n)S_n - t_n G)$$

Prouveur :
Construire P tel que $\forall j \neq i,\ P(j) = 0$

$$P(i) \neq 0 \quad \text{et} \quad P(0) = 1$$

- Soit (a_i) tel que $P = 1 + \sum_{k=1}^{n-1} a_k X^k$
- Soit (t_i) tel que $\xi_j = \begin{cases} 0 & \text{si } i \neq j \\ P(i)s_i \end{cases}$

Ainsi,

$$f(a_1, \ldots, a_{n-1}, t_1, \ldots, t_n) = (0, \ldots, 0)$$

Soit hash, fonction de hachage

Prouveur : Veux montrer que $f(x) = y$ sans donner x.
Soit R aléatoire,

$$A = f(R)$$

Soit

$$E = \text{hash}(A, \text{message-à-signer})$$
$$Z = E \times X + R$$

Le prouveur donne E et Z (pas d'info sur X grâce à R).
Vérifieur : il a donc E et Z (f et y sont publics).
Il calcule :

$$\text{hash}(f(Z) - E \times y, \text{message-à-signer})$$

Si c'est égal à E, alors le prouveur dit vrai.
Car :

$$f(Z) - E \times y = f(E \times X + R) - E \times y = E \times f(X) + f(R) - E \times y$$

$$= E \times y + A - E \times y = A$$

On choisit G comme un point sur la courbe elliptique, et on choisit la clef privée comme étant un scalaire clef privée $\times G$ = clef publique
Ici multiplier un élément du groupe G par un scalaire revient à trouver un autre point de la courbe elliptique qui sera la clef publique H_i
Je met ou la fonction de hashage?
H_i $\times$clef privée -> 2ème clef publique dépendant de i != ma clef publique

$$\forall i \in \{1, \ldots, n\}$$

$$\forall j \in \{1, \ldots, n\}\text{avec j != i}$$

H_i!=H_j Mais si deux signatures alors on peut remarquer que H_i est utilisé deux fois