Algorithm 
$$gen(1^k)$$
:

 $\begin{array}{l} \text{sample } \alpha \in \mathbb{Z}_n \\ \text{sample } \beta \in \mathbb{Z}_n^* \\ a := g^{\alpha} \\ b := g^{\beta} \\ sk := \alpha \| \beta \\ pk := a \| b \\ \mathbf{return } (sk, pk) \end{array}$ 

Algorithm  $sgn(sk, m)$ :

 $\begin{array}{l} \text{unpack } sk =: \alpha \| \beta \\ \mathbf{return } \frac{\alpha - m}{\beta} \end{array}$ 

Algorithm  $vert(pk, m, \sigma)$ :

 $\begin{array}{l} \text{unpack } pk := a \| b \\ \mathbf{return } a \stackrel{?}{=} g^m \cdot b^{\sigma} \end{array}$