Algorithm gen(1<sup>k</sup>):

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

Algorithm sgn(sk, m):

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

Algorithm vrf(pk, m, \sigma):

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