

Algorithm $\text{gen}(1^k)$:

sample $\alpha \in \mathbb{Z}_n$

sample $\beta \in \mathbb{Z}_n^*$

$a := g^\alpha$

$b := g^\beta$

$sk := \alpha || \beta$

$pk := a || b$

return (sk, pk)

Algorithm $\text{sgn}(sk, m)$:

unpack $sk =: \alpha || \beta$

return $\frac{\alpha - m}{\beta}$

Algorithm $\text{vrf}(pk, m, \sigma)$:

unpack $pk =: a || b$

return $a \stackrel{?}{=} g^m \cdot b^\sigma$