```
Algorithm gen($1^k$):
    sample $\alpha \in \mathbb{Z}_p$
    sample $\beta \in \mathbb{Z}_p^*$
    $a := g^\alpha$
    $b := g^\beta$
    $sk := \alpha \| \beta$
    $pk := a \| b$
    return $(sk, pk)$
```

```
Algorithm sgn($sk, m$):
    unpack $sk =: \alpha \| \beta$
    return $\frac{m-\alpha}{\beta}$
```

```
Algorithm vrf($pk, m, \sigma$):
    unpack $pk =: a \| b$
    return $g^m \overset{?}{=} a \cdot b^\sigma$
```