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

sample primes $p, q \in [2^k, 2^{k+1})$
$n := pq$
sample $a, b \in \mathbb{Z}_n$
sample $e \in \mathbb{Z}^*_{\phi(n)}$
$d := e^{-1} \pmod{\phi(n)}$
$sk := d \| a \| b$
$pk := e \| a \| b$
return (sk, pk)

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

unpack $sk =: d \| a \| b$
return $\left(\frac{a}{b^m}\right)^d$

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

unpack $pk =: e \| a \| b$
return $b^m \sigma^e \stackrel{?}{=} a$