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

Algorithm vrf(pk, m, σ):
- unpack $pk =: a\|b$
- **return** $b^m \sigma^e \overset{?}{=} a$