

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

**for**  $i = 1 \dots k$  **do**

sample  $r_i^0 \in \{0, 1\}^k$

sample  $r_i^1 \in \{0, 1\}^k$

compute  $f_i^0 := f(r_i^0)$

compute  $f_i^1 := f(r_i^1)$

$sk := \begin{pmatrix} r_1^0 & r_2^0 & \dots & r_k^0 \\ r_1^1 & r_2^1 & \dots & r_k^1 \end{pmatrix}$

$pk := \begin{pmatrix} f_1^0 & f_2^0 & \dots & f_k^0 \\ f_1^1 & f_2^1 & \dots & f_k^1 \end{pmatrix}$

**return**  $(sk, pk)$

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

unpack  $sk =: \begin{pmatrix} r_1^0 & r_2^0 & \dots & r_k^0 \\ r_1^1 & r_2^1 & \dots & r_k^1 \end{pmatrix}$

unpack  $m =: b_1 \| b_2 \| \dots \| b_k$

**return**  $r_1^{b_1} \| r_2^{b_2} \| \dots \| r_k^{b_k}$

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

unpack  $pk =: \begin{pmatrix} f_1^0 & f_2^0 & \dots & f_k^0 \\ f_1^1 & f_2^1 & \dots & f_k^1 \end{pmatrix}$

unpack  $m =: b_1 \| b_2 \| \dots \| b_k$

**return**  $\bigwedge_{i=1}^k (f(\sigma_i) = f_i^{b_i})$