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

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

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

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

return (sk, pk)

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

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

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

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

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

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

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

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