Signing Key: $\widehat{\mathbf{s}} \xleftarrow{\$} D_s^m$
Verification Key: $h \xleftarrow{\$} \mathcal{H}(R, D, m), \mathbf{S} \leftarrow h(\widehat{\mathbf{s}})$
Random Oracle: $\mathrm{H} : \{0,1\}^* \rightarrow D_c$

Sign$(\mu, h, \widehat{\mathbf{s}})$
1: $\widehat{\mathbf{y}} \xleftarrow{\$} D_y^m$
2: $\mathbf{e} \leftarrow \mathrm{H}(h(\widehat{\mathbf{y}}), \mu)$
3: $\widehat{\mathbf{z}} \leftarrow \widehat{\mathbf{s}}\mathbf{e} + \widehat{\mathbf{y}}$
4: if $\widehat{\mathbf{z}} \notin \mathrm{G}^m$, then goto step 1
5: output $(\widehat{\mathbf{z}}, \mathbf{e})$

Verify$(\mu, \widehat{\mathbf{z}}, \mathbf{e}, h, \mathbf{S})$
1: Accept iff
$\widehat{\mathbf{z}} \in \mathrm{G}^m$ and $\mathbf{e} = \mathrm{H}(h(\widehat{\mathbf{z}}) - \mathbf{S}\mathbf{e}, \mu)$