



$\mathcal{G}^{\mathcal{A}}$

[$(sk, pk) \leftarrow \text{Gen}$
 $sk^* \leftarrow \mathcal{A}(pk)$
return $[sk \stackrel{?}{=} sk^*]$]