



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

$$\left[\begin{array}{l} (sk, pk) \leftarrow \text{Gen} \\ sk^* \leftarrow \mathcal{A}^{\text{Enc}_{pk}(\cdot)}(pk) \\ \text{return } [sk \stackrel{?}{=} sk^*] \end{array} \right]$$