$(pk, sk) \leftarrow Gen(1^k)$