

secret key:  $\mathbf{s} \in \{0, 1\}^n$