Device [DB: secret $\mathbf{s}$] **Server** [DB: secret $\mathbf{s}$]

$$(\mathbf{a}_i, b_i) \leftarrow A_{\mathbf{s}, \bar{\Psi}_\alpha}, \ i = 1, 2..., m$$

$$r \leftarrow \{0, 1\}$$

$$S \leftarrow \mathfrak{P}(\{1, 2, \ldots, m\})$$

$$c = (\mathbf{a}, b + \lfloor q/2 \rfloor r) = (\sum_{i \in S} \mathbf{a}_i, \sum_{i \in S} b_i + \lfloor q/2 \rfloor r)$$

$$\xleftarrow{\quad c \quad}$$

$r' \leftarrow \text{LPUF}(c)$

$$\xrightarrow{\quad r' \quad}$$

accept if $r = r'$