$$\mathbf{s} \leftarrow \mathrm{POK}$$

$$\rightarrow$$
  $\mathbf{h} \leftarrow \text{FE.Gen}(\mathbf{s})$ 

$$\mathbf{E} \leftarrow \bar{\Psi}_{\alpha}$$

$$\mathbf{r} \leftarrow \text{TRNG}()$$

$$seed_{\mathbf{a}'} \leftarrow TRNG()$$

$$\mathbf{X} \leftarrow \mathrm{TRNG}()$$

$$\mathbf{b'} \leftarrow \text{LFSR}(\text{seed}_{\mathbf{a'}})^T \mathbf{s} + \mathbf{E}^T \mathbf{X} + \mathbf{r} \lfloor q/2 \rfloor$$

$$ch \leftarrow (\operatorname{seed}_{\mathbf{a}'}, \mathbf{b}')$$

$$DB = (\mathbf{s}, \mathbf{h}, \mathbf{E}, ch, \mathbf{r})$$

$$\mathbf{s}_R \leftarrow \mathrm{POK}$$

$$\underline{\mathbf{h}, ch}$$
  $\mathbf{h}, ch \leftarrow \mathrm{DB}$ 

$$\mathbf{s} \leftarrow \mathrm{FE.Rec}(\mathbf{s_R}, \mathbf{h})$$

$$\mathbf{r}_R \leftarrow \mathrm{PUF}(ch, \mathbf{s})$$

$$\longrightarrow$$
 accept if  $HD(\mathbf{r}_R, \mathbf{r}) < th$