Device		Server
Enroll.$(1\times)$		
$\mathbf{s} \leftarrow \mathrm{POK}$	$\xrightarrow{\mathbf{s}}$	$\mathbf{h} \leftarrow \mathrm{FE.Gen}(\mathbf{s})$
		$\mathbf{E} \leftarrow \bar{\Psi}_\alpha$
		$\mathbf{r} \leftarrow \mathrm{TRNG}()$
		$\mathrm{seed}_{\mathbf{a}'} \leftarrow \mathrm{TRNG}()$
		$\mathbf{X} \leftarrow \mathrm{TRNG}()$
		$\mathbf{b}' \leftarrow \mathrm{LFSR}(\mathrm{seed}_{\mathbf{a}'})^T\mathbf{s} + \mathbf{E}^T\mathbf{X} + \mathbf{r}\lfloor q/2 \rfloor$
		$ch \leftarrow (\mathrm{seed}_{\mathbf{a}'}, \mathbf{b}')$
		$\mathrm{DB} = (\mathbf{s}, \mathbf{h}, \mathbf{E}, ch, \mathbf{r})$
Authenticate.(∞)		
$\mathbf{s}_R \leftarrow \mathrm{POK}$	$\xleftarrow{\mathbf{h}, ch}$	
$\mathbf{s} \leftarrow \mathrm{FE.Rec}(\mathbf{s_R}, \mathbf{h})$		
$\mathbf{r}_R \leftarrow \mathrm{PUF}(ch, \mathbf{s})$	$\xrightarrow{\mathbf{r}_R}$	accept if $\mathrm{HD}(\mathbf{r}_R, \mathbf{r}) < th$