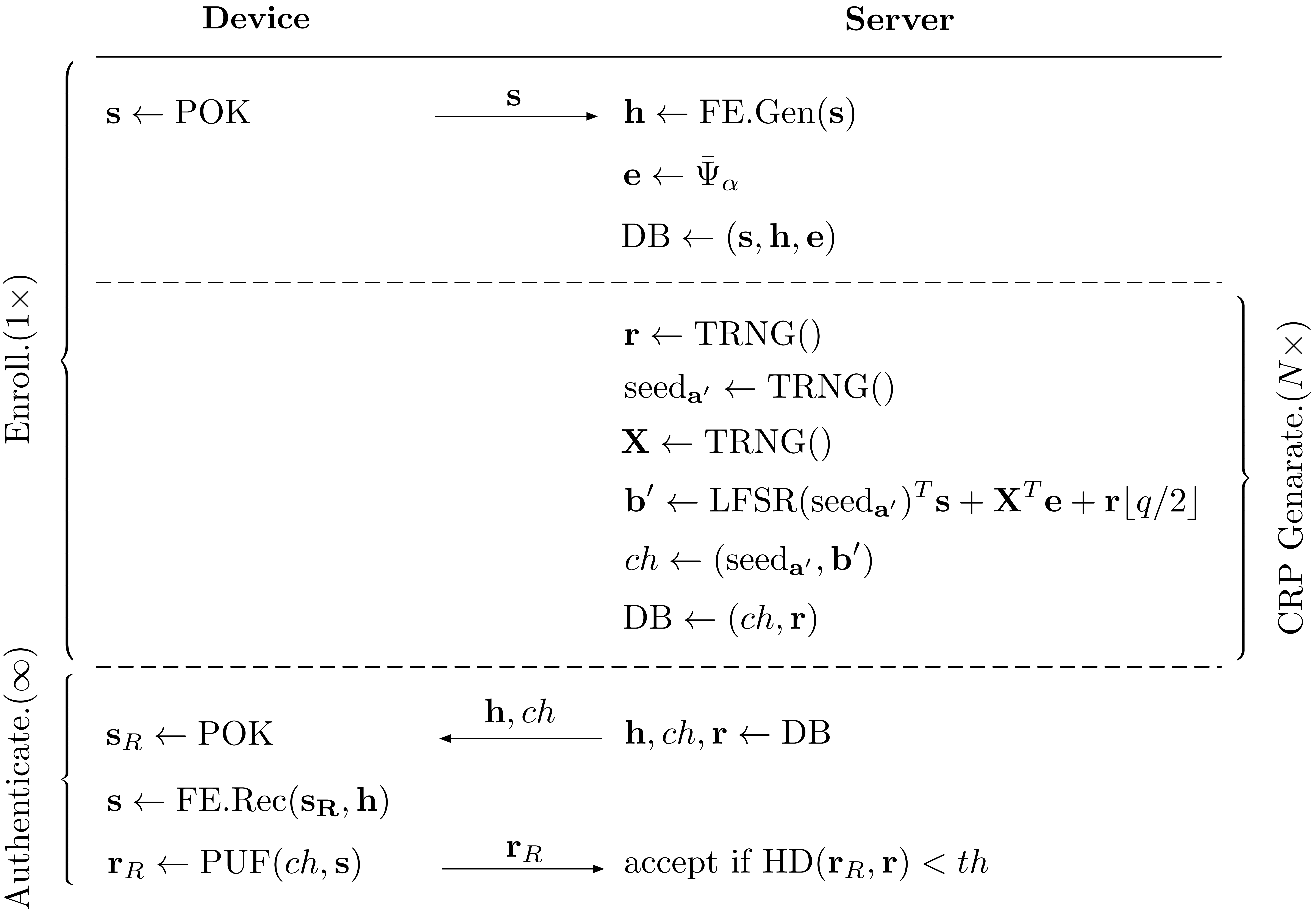

Device
Server
Enroll.$(1\times)$
$\mathbf{s} \leftarrow \mathrm{POK}$
$\mathbf{s}$
$\mathbf{h} \leftarrow \mathrm{FE.Gen}(\mathbf{s})$
$\mathbf{e} \leftarrow \bar{\Psi}_\alpha$
$\mathrm{DB} \leftarrow (\mathbf{s}, \mathbf{h}, \mathbf{e})$
CRP Genarate.$(N\times)$
$\mathbf{r} \leftarrow \mathrm{TRNG}()$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