| | Used for ... | Keys or Functions |
|---|---|---|
| Advanced | linear transformation | $\mathsf{gemv}(\boldsymbol{A}, \mathsf{ct}, \mathsf{rk})$, $\mathsf{sum}(\mathsf{ct}, \mathsf{rk})$, $\mathsf{idx}(\mathsf{ct}, i, \mathsf{rk})$<br>$\mathsf{nrm22}(\mathsf{ct}, \mathsf{rlk}, \mathsf{rk}, \mathsf{ck})$ |
| | nonlinear functions | $\exp(\mathsf{ct}, \mathsf{rlk})$, $\ln(\mathsf{ct}, \mathsf{rlk})$, $\mathsf{sigmoid}(\mathsf{ct}, \mathsf{rlk})$ |
| | Comparison | $\mathsf{inv}(\mathsf{ct}, \mathsf{rlk}, d)$, $\mathsf{sqrt}(\mathsf{ct}, \mathsf{rlk}, d)$, $\mathsf{cmp}(\mathsf{ct}_1, \mathsf{ct}_2, \mathsf{rlk}, d, \alpha)$ |
| Primitives | addition | $\mathsf{add}_{\mathsf{pt}}(\mathsf{ct}, \mathsf{pt})$, $\mathsf{add}(\mathsf{ct}_1, \mathsf{ct}_2)$, $\mathsf{neg}(\mathsf{ct})$<br>$\mathsf{sub}_{\mathsf{pt}}(\mathsf{ct}, \mathsf{pt})$, $\mathsf{sub}(\mathsf{ct}_1, \mathsf{ct}_2)$ |
| | level switch | $\mathsf{rs}_{\ell \to \ell'}(\mathsf{ct})$, $\mathsf{moddown}_{\ell \to \ell'}(\mathsf{ct})$ |
| | multiplication | $\mathsf{mult}_{\mathsf{pt}}(\mathsf{ct}, \mathsf{pt})$, $\mathsf{mult}(\mathsf{ct}_1, \mathsf{ct}_2, \mathsf{rlk})$ |
| | automorphism | $\mathsf{rot}(\mathsf{ct}, r, \mathsf{rk})$, $\mathsf{conj}(\mathsf{ct}, \mathsf{ck})$ |
| Encryptor | encrypt/decrypt | $\mathsf{ct} = \mathsf{enc}_{\mathsf{pk}/\mathsf{sk}}(\mathsf{pt}, \mathsf{pk}/\mathsf{sk})$, $\mathsf{pt} = \mathsf{dec}(\mathsf{ct}, \mathsf{sk})$ |
| Encoder | encode/decode | $\mathsf{pt} = \mathsf{ecd}(\boldsymbol{z}, \Delta)$, $\boldsymbol{z} = \mathsf{dcd}(\mathsf{pt}, \Delta)$ |
| KEM | public key, secret key | $\mathsf{pk}, \mathsf{sk} = \mathsf{keypair}(\mathsf{ctx})$ |
| | evaluation keys | $\mathsf{rlk} = \mathsf{genswk}(\mathsf{sk} \cdot \mathsf{sk}, \mathsf{sk})$<br>$\mathsf{rk}_r = \mathsf{genswk}(\tau_{5^r \bmod 2n}(\mathsf{sk}), \mathsf{sk}), 0 \leq r < \cdots n_{\mathsf{slots}}$<br>$\mathsf{ck} = \mathsf{genswk}(\tau_{-1}(\mathsf{sk}), \mathsf{sk})$ |