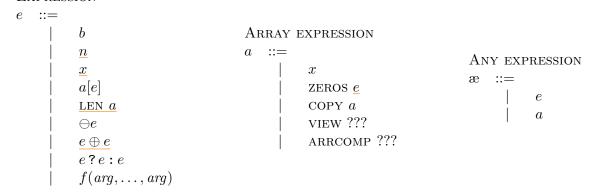
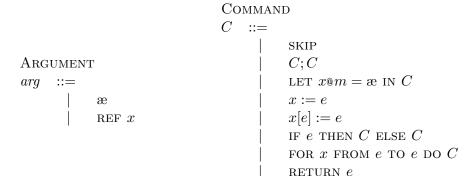
Grammar

EXPRESSION





Function definition $f ::= \text{ func } f(x @ \tau, \cdots, x @ \tau) : t \{C\}$

Type Lattice

$$\frac{\ell_1 \sqsubseteq \ell_2}{\text{Public} \sqsubseteq \text{Secret}} \qquad \frac{\ell_1 \sqsubseteq \ell_2}{\beta_{\ell_1}^m \sqsubseteq \beta_{\ell_2}^{\text{Const}}} \qquad \frac{\ell_1 \sqsubseteq \ell_2}{\text{Arr}[\beta, \underline{e}]_{\ell_1}^{\text{Mut}} \sqsubseteq \text{Arr}[\beta, \underline{e}]_{\ell_2}^{\text{Const}}}$$

$$\frac{\Gamma \vdash e : \tau_1 \qquad \tau_1 \sqsubseteq \tau_2}{\Gamma \vdash e : \tau_2}$$

Expressions

$$\begin{array}{c|c} \hline \text{Expressions} & \hline \Gamma \vdash a : \text{DOOL}_{\text{PUBLIC}}^{\text{CONST}} & \hline \Gamma \vdash h : \text{INT}_{\text{PUBLIC}}^{\text{CONST}} & \hline \Gamma(x) = \beta_{\ell}^{m} \\ \hline \Gamma \vdash b : \text{BOOL}_{\text{PUBLIC}}^{\text{CONST}} & \hline \Gamma \vdash h : \text{INT}_{\text{PUBLIC}}^{\text{CONST}} & \hline \Gamma \vdash a : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash a : \text{ARR}[\beta, \underline{ea}]_{\ell}^{m} & \text{SMT}(0 \leq e < e_{a}) & \hline \Gamma \vdash a : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash \text{LEN } a : \text{INT}_{\text{PUBLIC}}^{\text{CONST}} \\ \hline \hline \Gamma \vdash e : t_{1} & \oplus : t_{1} \rightarrow t_{2} \\ \hline \Gamma \vdash \theta e : t_{2} & \hline \Gamma \vdash e_{1} : t_{1} & \Gamma \vdash e_{2} : t_{2} & \oplus : t_{1} \rightarrow t_{2} \rightarrow t_{3} \\ \hline \Gamma \vdash e_{1} : \text{BOOL}_{\ell}^{\text{CONST}} & \Gamma \vdash e_{2} : \beta_{\ell}^{\text{CONST}} & \Gamma \vdash e_{3} : \beta_{\ell}^{\text{CONST}} \\ \hline \Gamma \vdash e_{1} : e_{2} : e_{3} : \beta_{\ell}^{\text{CONST}} & \Gamma \vdash e_{3} : \beta_{\ell}^{\text{CONST}} \\ \hline \Gamma \vdash e_{1} : e_{2} : e_{3} : \beta_{\ell}^{\text{CONST}} & \text{if } arg_{i} = \varpi_{i} \\ \hline \Gamma \vdash f(arg_{1}, \dots, arg_{n}) : \beta_{\ell}^{\text{CONST}} & \text{if } arg_{i} = \text{REF } x_{i} \\ \hline \Gamma \vdash \text{COPY } a : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} & \hline \Gamma \vdash a : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash \text{VIEW } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash \text{VIEW } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash \text{VIEW } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash \text{COPY } a : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} & \hline \Gamma \vdash \text{VIEW } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash \text{VIEW } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} & \hline \Gamma \vdash \text{VIEW } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash \text{VIEW } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{m} \\ \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} & \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} \\ \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} & \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} \\ \hline \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} & \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} \\ \hline \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} & \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} \\ \hline \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} & \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} \\ \hline \hline \Gamma \vdash \text{ARRCOMP } ??? : \text{ARR}[\beta, \underline{e}]_{\ell}^{\text{MUT}} & \hline \Gamma \vdash \text{ARRCOMP } ?? : \text{ARRCOMP } ?? : \text{ARRCO$$

 $\boxed{\Gamma \vdash^{rp}_{pc} C : rp}$ Statements

$$\frac{\Gamma \stackrel{lTp}{pc} C_1 : rp' \qquad \Gamma \stackrel{lTp}{pc} C_2 : rp''}{\Gamma \stackrel{lTp}{pc} C_1 : rp' \qquad \Gamma \stackrel{lTp}{pc} C_2 : rp''}$$

$$\frac{\Gamma \vdash e : \beta_{\ell}^{\text{Const}} \qquad \ell \sqcup pc \sqsubseteq \ell' \qquad \Gamma[x \mapsto \beta_{\ell'}^m] \stackrel{lTp}{pc} C : rp'}{\Gamma \stackrel{lTp}{pc} \text{ Let } x@m = e \text{ in } C : rp'}$$

$$\frac{\Gamma(x) = \beta_{\ell}^{\text{Mut}} \qquad \Gamma \vdash e : \beta_{\ell}^{\text{Const}} \qquad rp \sqcup pc \sqsubseteq \ell}{\Gamma \stackrel{lTp}{pc} x := e : rp}$$

$$\frac{\Gamma(x) = \text{Arr} \left[\beta, e_a\right]_{\ell}^{\text{Mut}} \qquad \text{SMT} (0 \le e_1 < e_a) \qquad \Gamma \vdash e_2 : \beta_{\ell}^{\text{Const}} \qquad rp \sqcup pc \sqsubseteq \ell}{\Gamma \stackrel{lTp}{pc} x [e_1] := e_2 : rp}$$

$$\frac{\Gamma \vdash e : \text{Bool}_{\ell}^{\text{Const}} \qquad pc' = pc \sqcup \ell \qquad \Gamma \stackrel{lTp}{pc'} C_1 : rp_1 \qquad \Gamma \stackrel{lTp}{pc'} C_2 : rp_2}{\Gamma \stackrel{lTp}{pc'} \text{ If } e \text{ THEN } C_1 \text{ ELSE } C_2 : rp_1 \sqcup rp_2}$$

$$\frac{\Gamma \vdash e : \mathrm{Bool}^{\mathrm{Const}}_{\ell} \quad pc' = pc \sqcup \ell \quad \Gamma \vdash^{rp}_{pc'} C_1 : rp_1 \quad \Gamma \vdash^{rp}_{pc'} C_2 : rp_2}{\Gamma \vdash^{rp}_{pc} \text{ if } e \text{ then } C_1 \text{ else } C_2 : rp_1 \sqcup rp_2}$$

$$\frac{\Gamma \vdash e_1 : \operatorname{Int}^{\operatorname{Const}}_{\operatorname{Public}} \quad \Gamma \vdash e_2 : \operatorname{Int}^{\operatorname{Const}}_{\operatorname{Public}} \quad \Gamma[x \mapsto \operatorname{Int}^{\operatorname{Const}}_{\operatorname{Public}}] \stackrel{t^{xp}}{\not\models_{pc}} C : rp'}{\Gamma \mid_{pc}^{t^p} \text{ for } x \text{ from } e_1 \text{ to } e_2 \text{ do } C : rp'}$$

$$\frac{\Gamma(rval) = \beta_{\ell}^{\text{Const}} \qquad \Gamma \vdash e : \beta_{\ell}^{\text{Const}} \qquad rp \sqcup pc \sqsubseteq \ell}{\Gamma \vdash_{pc}^{pc} \text{ return } e : rp \sqcup pc}$$