Grammar

Base type
$$\beta ::= \mid \textsc{Bool} \mid \textsc{Int}$$

Array type
$$\alpha ::= \textsc{Arr}[\beta, \underline{e}]$$

Label
$$\ell, pc, rp ::= \mid \textsc{Public} \mid \textsc{Secret}$$

Mutability
$$m ::= \mid \textsc{Const} \mid \textsc{Mut}$$

Base type tuple
$$t ::= \beta^m_\ell$$

Type tuple
$$\tau ::= \mid \beta^m_\ell \mid \alpha^m_\ell$$

Expression
$$e ::= \mid b \mid \underline{n} \mid \underline{x} \mid a[e] \mid \underline{\text{LEN } a} \mid \ominus e \mid \underline{e \oplus e} \mid e \,?\, e : e \mid f(arg, \ldots, arg)$$

Array expression
$$a ::= \mid x \mid \text{ZEROS } \underline{e} \mid \text{COPY } a \mid \text{VIEW ???} \mid \text{ARRCOMP ???}$$

Any expression
$$æ ::= \mid e \mid a$$

Argument
$$arg ::= \mid æ \mid \text{REF } x$$

Command
$$C ::= \mid \text{SKIP} \mid C; C \mid \text{LET } x@m = æ \text{ IN } C \mid x := e \mid x[e] := e \mid \text{IF } e \text{ THEN } C \text{ ELSE } C \mid \text{FOR } x \text{ FROM } e \text{ TO } e \text{ DO } C \mid \text{RETURN } e$$

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

Type Lattice

$$\frac{}{\textsc{Public} \sqsubset \textsc{Secret}} \qquad \frac{\ell_1 \sqsubseteq \ell_2}{\beta^m_{\ell_1} \sqsubset \beta^{\textsc{Const}}_{\ell_2}} \qquad \frac{\ell_1 \sqsubseteq \ell_2}{\textsc{Arr}[\beta, \underline{e}]^{\textsc{Mut}}_{\ell_1} \sqsubset \textsc{Arr}[\beta, \underline{e}]^{\textsc{Const}}_{\ell_2}}$$

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

Expressions $\boxed{\Gamma \vdash æ : \tau}$

$$\frac{}{\Gamma \vdash b : \textsc{Bool}^{\textsc{Const}}_{\textsc{Public}}} \qquad \frac{}{\Gamma \vdash n : \textsc{Int}^{\textsc{Const}}_{\textsc{Public}}} \qquad \frac{\Gamma(x) = \beta^m_\ell}{\Gamma \vdash x : \beta^{\textsc{Const}}_\ell}$$

$$\frac{\Gamma \vdash a : \textsc{Arr}\big[\beta, \underline{e_a}\big]^m_\ell \qquad \mathrm{SMT}(0 \leq e < e_a)}{\Gamma \vdash a[e] : \beta^{\textsc{Const}}_\ell} \qquad \frac{\Gamma \vdash a : \textsc{Arr}[\beta, \underline{e}]^m_\ell}{\Gamma \vdash \textsc{len}\ a : \textsc{Int}^{\textsc{Const}}_{\textsc{Public}}}$$

$$\frac{\Gamma \vdash e : t_1 \qquad \ominus : t_1 \to t_2}{\Gamma \vdash \ominus e : t_2} \qquad \frac{\Gamma \vdash e_1 : t_1 \qquad \Gamma \vdash e_2 : t_2 \qquad \oplus : t_1 \to t_2 \to t_3}{\Gamma \vdash e_1 \oplus e_2 : t_3}$$

$$\frac{\Gamma \vdash e_1 : \textsc{Bool}^{\textsc{Const}}_\ell \qquad \Gamma \vdash e_2 : \beta^{\textsc{Const}}_\ell \qquad \Gamma \vdash e_3 : \beta^{\textsc{Const}}_\ell}{\Gamma \vdash e_1 \,\textbf{?}\, e_2 : e_3 : \beta^{\textsc{Const}}_\ell}$$

$$\frac{\Gamma(f) = \prod_{i=1}^{n} \beta^{m_i}_{i_{\ell_i}} \to \beta^{\textsc{Const}}_\ell \qquad \bigwedge_{i=1}^{n} \begin{cases} \Gamma \vdash \ell_i : \beta^{\textsc{Const}}_{i_{\ell_i}} & \text{if } \mathit{arg}_i = æ_i \\ \Gamma \vdash x_i : \beta^{\textsc{Mut}}_{i_{\ell_i}} & \text{if } \mathit{arg}_i = \textsc{ref}\ x_i \end{cases}}{\Gamma \vdash f(\mathit{arg}_1, \ldots, \mathit{arg}_n) : \beta^{\textsc{Const}}_\ell}$$

$$\frac{}{\Gamma \vdash \textsc{zeros}_\ell\ \underline{e} : \textsc{Arr}[\textsc{Int}, \underline{e}]^{\textsc{Mut}}_\ell} \qquad \frac{\Gamma \vdash a : \textsc{Arr}[\beta, \underline{e}]^m_\ell}{\Gamma \vdash \textsc{copy}\ a : \textsc{Arr}[\beta, \underline{e}]^{\textsc{Mut}}_\ell} \qquad \frac{\Gamma \vdash a : \textsc{Arr}[\beta, \underline{e}]^m_\ell}{\Gamma \vdash \textsc{view}\ ??? : \textsc{Arr}\big[\beta, \underline{e'}\big]^m_\ell}$$

$$\frac{???}{\Gamma \vdash \textsc{arrcomp}\ ??? : \textsc{Arr}[\beta, \underline{e}]^{\textsc{Mut}}_\ell}$$

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

$$\frac{}{\Gamma \vdash^{rp}_{pc} \text{SKIP} : rp} \qquad \frac{\Gamma \vdash^{rp}_{pc} C_1 : rp' \qquad \Gamma \vdash^{rp'}_{pc} C_2 : rp''}{\Gamma \vdash^{rp}_{pc} C_1; C_2 : rp''}$$

$$\frac{\Gamma \vdash e : \beta^{\text{Const}}_{\ell} \qquad \ell \sqcup pc \sqsubseteq \ell' \qquad \Gamma[x \mapsto \beta^{m}_{\ell'}] \vdash^{rp}_{pc} C : rp'}{\Gamma \vdash^{rp}_{pc} \text{LET } x@m = e \text{ IN } C : rp'}$$

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

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

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

$$\frac{\Gamma \vdash e_1 : \text{Int}^{\text{Const}}_{\text{Public}} \qquad \Gamma \vdash e_2 : \text{Int}^{\text{Const}}_{\text{Public}} \qquad \Gamma[x \mapsto \text{Int}^{\text{Const}}_{\text{Public}}] \vdash^{rp}_{pc} C : rp'}{\Gamma \vdash^{rp}_{pc} \text{FOR } x \text{ FROM } e_1 \text{ TO } e_2 \text{ DO } C : rp'}$$

$$\frac{\Gamma(rval) = \beta^{\text{Const}}_{\ell} \qquad \Gamma \vdash e : \beta^{\text{Const}}_{\ell} \qquad rp \sqcup pc \sqsubseteq \ell}{\Gamma \vdash^{rp}_{pc} \text{RETURN } e : rp \sqcup pc}$$