Grammar

Base type
β ::=
| Bool
| Int

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

Label
ℓ, pc, rp ::=
| Public
| Secret

Mutability
m ::=
| Const
| Mut

Base type tuple
t ::= β_ℓ^m

Type tuple
τ ::=
| β_ℓ^m
| α_ℓ^m

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

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

Any expression
æ ::=
| e
| a

Argument
arg ::=
| æ
| REF x

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

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

Type Lattice

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\frac{\Gamma \vdash e_1 : \textsc{Int}_{\textsc{Public}}^{\textsc{Const}} \qquad \Gamma \vdash e_2 : \textsc{Int}_{\textsc{Public}}^{\textsc{Const}} \qquad \Gamma[x \mapsto \textsc{Int}_{\textsc{Public}}^{\textsc{Const}}] \vdash^{rp}_{pc} C : rp'}{\Gamma \vdash^{rp}_{pc} \textsc{for}\ x\ \textsc{from}\ e_1\ \textsc{to}\ e_2\ \textsc{do}\ C : rp'}$$

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