Grammar

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Base type}} \\ b & ::= & \\ & | & \textsc{Bool} \\ & | & \textsc{UInt}_n \\ & | & \textsc{Int}_n \end{array}$$

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Type}} \\ \tau & ::= & \\ & | & b \\ & | & \textsc{Ref}\langle b \rangle \\ & | & \textsc{Arr}\langle b, n \rangle \\ & | & \textsc{Arr}\langle b, x \rangle \quad x \text{ must be } \langle \textsc{Ref}\langle \textsc{UInt} \rangle, \textsc{Public}, \textsc{Const} \rangle \end{array}$$

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Label}} \\ \ell & ::= & \\ & | & \textsc{Public} \\ & | & \textsc{Secret} \end{array}$$

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Variable label}} \\ \ell^x & ::= & \\ & | & \ell \\ & | & \textsc{FlowS}\langle \ell \rangle \end{array}$$

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Mutability}} \\ \sigma & ::= & \\ & | & \textsc{Const} \\ & | & \textsc{Mut} \end{array}$$

$$\begin{array}{llll} \multicolumn{4}{l}{\textsc{Expression}} \\ e & ::= & & \\ & | & \textsc{true} & \\ & | & \textsc{false} & \\ & | & c & \text{integer literal} \\ & | & x & \text{variable} \\ & | & x[e] & \text{array get} \\ & | & \langle b, n, b_x \rangle x \Rightarrow e & \text{array comprehension} \\ & | & \textsc{view}(x, e, n) & \text{array view} \\ & | & \ominus e & \text{unary op} \\ & | & e_1 \oplus e_2 & \text{binary op} \\ & | & e_1 \, \mathbf{?} \, e_2 : e_3 & \text{ternary op} \\ & | & \textsc{ref } x & \text{mut ref} \\ & | & f(e_1, \ldots, e_n) & \text{function call} \end{array}$$

$$\begin{array}{llll} \multicolumn{4}{l}{\textsc{Statement}} \\ s & ::= & & \\ & | & \diamond & \text{empty} \\ & | & s_1; s_2 & \text{sequence} \\ & | & \langle \textsc{Ref}\langle b \rangle, \sigma \rangle x = e & \text{variable declaration} \\ & | & \langle \textsc{Arr}\langle b, n \rangle, \ell, \sigma \rangle x = e & \text{array declaration} \\ & | & x := e & \text{variable assignment} \\ & | & x[e_1] := e_2 & \text{array assignment} \\ & | & \textsc{if } e \ \{s_1\} \ \textsc{else} \ \{s_2\} & \text{conditional} \\ & | & \textsc{for } \langle b \rangle x \ \textsc{from } e_1 \ \textsc{to } e_2 \ \{s\} & \text{loop} \\ & | & \textsc{return } e & \text{return} \end{array}$$

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Function Definition}} \\ fdec & ::= & \\ & | & \langle b, \ell \rangle f(\langle \tau_1, \ell_1, \sigma_1 \rangle x_1, \ \ldots \ , \langle \tau_n, \ell_n, \sigma_n \rangle x_n) \ \{s\} \end{array}$$

Metavariables

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Type context}} \\ \Gamma & ::= & \\ & | & \emptyset \\ & | & \Gamma[e \mapsto \langle \tau, \ell, \sigma \rangle] \end{array} \qquad \begin{array}{lll} \multicolumn{3}{l}{\textsc{Variable type store}} \\ \mu & ::= & \\ & | & \emptyset \\ & | & \mu[x \mapsto \langle \tau, \ell^x, \sigma \rangle] \end{array}$$

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Function type store}} \\ \mathbb{F} & ::= & \\ & | & \emptyset \\ & | & \mathbb{F}[f \mapsto fdec(\langle \tau_1, \ell_1, \sigma_1 \rangle, \ldots, \langle \tau_n, \ell_n, \sigma_n \rangle) : \langle b, \ell \rangle] \end{array}$$

Type Lattice

$$\frac{n_1 < n_2}{\textsc{UInt}_{n_1} \sqsubset \textsc{UInt}_{n_2}} \qquad \frac{n_1 < n_2}{\textsc{Int}_{n_1} \sqsubset \textsc{Int}_{n_2}} \qquad \frac{}{\textsc{UInt}_{n} \sqsubset \textsc{Int}_{2n}} \qquad \frac{}{\textsc{Public} \sqsubset \textsc{Secret}}$$

$$\frac{}{\textsc{Mut} \sqsubset \textsc{Const}} \qquad \frac{\Gamma \,|\, \mu \vdash e : \langle b, \ell, \textsc{Const} \rangle \qquad b \sqsubseteq b' \qquad \ell \sqsubseteq \ell'}{\Gamma \,|\, \mu \vdash e : \langle b', \ell', \textsc{Const} \rangle}$$

$$\frac{\Gamma \,|\, \mu \vdash e : \langle \textsc{Arr}\langle b, n \rangle, \ell, \sigma \rangle \qquad \ell \sqsubseteq \ell'}{\Gamma \,|\, \mu \vdash e : \langle \textsc{Arr}\langle b, n \rangle, \ell', \textsc{Const} \rangle} \qquad \frac{\Gamma \,|\, \mu \vdash e : \langle \textsc{Arr}\langle b, x \rangle, \ell, \sigma \rangle \qquad \ell \sqsubseteq \ell'}{\Gamma \,|\, \mu \vdash e : \langle \textsc{Arr}\langle b, x \rangle, \ell', \textsc{Const} \rangle}$$

Expressions $\boxed{\Gamma \mid \mu \vdash e : \langle \tau, \ell, \sigma \rangle}$

Var
$$\frac{\mu(x) = \langle \textsc{Ref}\langle b \rangle, \ell^x, \sigma \rangle \qquad \ell^x = \ell' \text{ or } \ell^x = \textsc{FlowS}\langle \ell' \rangle}{\Gamma \mid \mu \vdash x : \langle b, \ell', \textsc{Const} \rangle}$$

ArrVar
$$\frac{\mu(x) = \langle \textsc{Arr}\langle b, n \rangle, \ell, \sigma \rangle}{\Gamma \mid \mu \vdash x : \langle \textsc{Arr}\langle b, n \rangle, \ell, \textsc{Const} \rangle}$$

Unop
$$\frac{\Gamma \mid \mu \vdash e : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \ominus : \langle \tau_1, \ell_1, \sigma_1 \rangle \to \langle \tau_2, \ell_2, \sigma_2 \rangle}{\Gamma \mid \mu \vdash \ominus e : \langle \tau_2, \ell_2, \sigma_2 \rangle}$$

Binop
$$\frac{\Gamma \mid \mu \vdash e_1 : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \Gamma \mid \mu \vdash e_2 : \langle \tau_2, \ell_2, \sigma_2 \rangle \qquad \oplus : \langle \tau_1, \ell_1, \sigma_1 \rangle \to \langle \tau_2, \ell_2, \sigma_2 \rangle \to \langle \tau_3, \ell_3, \sigma_3 \rangle}{\Gamma \mid \mu \vdash e_1 \oplus e_2 : \langle \tau_3, \ell_3, \sigma_3 \rangle}$$

Ternop
$$\frac{\begin{array}{c}\Gamma \mid \mu \vdash e_1 : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \Gamma \mid \mu \vdash e_2 : \langle \tau_2, \ell_2, \sigma_2 \rangle \\ \Gamma \mid \mu \vdash e_3 : \langle \tau_3, \ell_3, \sigma_3 \rangle \qquad (\,?\,:) : \langle \tau_1, \ell_1, \sigma_1 \rangle \to \langle \tau_2, \ell_2, \sigma_2 \rangle \to \langle \tau_3, \ell_3, \sigma_3 \rangle \to \langle \tau_4, \ell_4, \sigma_4 \rangle\end{array}}{\Gamma \mid \mu \vdash e_1 \,?\, e_2 : e_3 : \langle \tau_4, \ell_4, \sigma_4 \rangle}$$

ArrGet
$$\frac{\mu(x) = \langle \textsc{Arr}\langle b, n \rangle, \ell, \sigma \rangle \qquad \Gamma \mid \mu \vdash e : \langle \text{UInt}, \textsc{Public}, \textsc{Const} \rangle \qquad \mathit{SMT}(e < n)}{\Gamma \mid \mu \vdash x[e] : \langle b, \ell, \textsc{Const} \rangle}$$

ArrGetDyn
$$\frac{\mu(x) = \langle \textsc{Arr}\langle b, x_n \rangle, \ell, \sigma \rangle \qquad \Gamma \mid \mu \vdash e : \langle \text{UInt}, \textsc{Public}, \textsc{Const} \rangle \qquad \mathit{SMT}(e < x_n)}{\Gamma \mid \mu \vdash x[e] : \langle b, \ell, \textsc{Const} \rangle}$$

ArrComp
$$\frac{\Gamma \mid \mu[x \mapsto \langle b_x, \textsc{Public}, \textsc{Const} \rangle] \vdash e : \langle b, \ell, \textsc{Const} \rangle \qquad \text{UInt}_{\lceil \log_2 n \rceil} \sqsubseteq b_x}{\Gamma \mid \mu \vdash \langle b, n, b_x \rangle x \Rightarrow e : \langle \textsc{Arr}\langle b, n \rangle, \ell, \textsc{Mut} \rangle}$$

ArrView
$$\frac{\mu(x) = \langle \textsc{Arr}\langle b, n \rangle, \ell, \sigma \rangle \qquad \Gamma \mid \mu \vdash e : \langle \text{UInt}, \textsc{Public}, \textsc{Const} \rangle \qquad \mathit{SMT}(e + n' < n)}{\Gamma \mid \mu \vdash \textsc{view}(x, e, n') : \langle \textsc{Arr}\langle b, n' \rangle, \ell, \sigma \rangle}$$

ArrViewDyn
$$\frac{\mu(x) = \langle \textsc{Arr}\langle b, x_n \rangle, \ell, \sigma \rangle \qquad \Gamma \mid \mu \vdash e : \langle \text{UInt}, \textsc{Public}, \textsc{Const} \rangle \qquad \mathit{SMT}(e + n' < x_n)}{\Gamma \mid \mu \vdash \textsc{view}(x, e, n') : \langle \textsc{Arr}\langle b, n' \rangle, \ell, \sigma \rangle}$$

MutRef
$$\frac{\mu(x) = \langle \tau, \ell^x, \textsc{Mut} \rangle \qquad \ell^x = \ell' \text{ or } \ell^x = \textsc{FlowS}\langle \ell' \rangle}{\Gamma \mid \mu \vdash \textsc{ref}\ x : \langle \tau, \ell', \textsc{Mut} \rangle}$$

FnCall
$$\frac{\begin{array}{c}\mathbb{F}(f) = \mathit{fdec}(\langle \tau_1, \ell_1, \sigma_1 \rangle, \ldots, \langle \tau_n, \ell_n, \sigma_n \rangle) : \langle b, \ell \rangle \\ \Gamma \mid \mu \vdash e_1 : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \ldots \qquad \Gamma \mid \mu \vdash e_n : \langle \tau_n, \ell_n, \sigma_n \rangle\end{array}}{\Gamma \mid \mu \vdash f(e_1, \ldots, e_n) : \langle b, \ell, \textsc{Const} \rangle}$$

True
$$\frac{}{\Gamma \mid \mu \vdash \textsc{true} : \langle \textsc{Bool}, \textsc{Public}, \textsc{Const} \rangle}$$

False
$$\frac{}{\Gamma \mid \mu \vdash \textsc{false} : \langle \textsc{Bool}, \textsc{Public}, \textsc{Const} \rangle}$$

PosNumber
$$\frac{c >= 0 \qquad n = \lceil \log_2 c \rceil}{\Gamma \mid \mu \vdash c : \langle \text{UInt}_n, \textsc{Public}, \textsc{Const} \rangle}$$

NegNumber
$$\frac{c < 0 \qquad n = \lceil \log_2 |c| \rceil + 1}{\Gamma \mid \mu \vdash c : \langle \text{Int}_n, \textsc{Public}, \textsc{Const} \rangle}$$

Statements $\boxed{\Gamma \,|\, \mu \vdash_{pc} s}$

$$\textsc{Empty}\quad \frac{}{\Gamma \,|\, \mu \vdash_{pc} \diamond}$$

$$\textsc{VarDecBaseMut}\quad \frac{x \notin Dom(\mu) \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell, \textsc{Const}\rangle \qquad \Gamma \,|\, \mu[x \mapsto \langle \textsc{Ref}\langle b\rangle, \textsc{FlowS}\langle \ell\rangle, \textsc{Mut}\rangle] \vdash_{pc} s}{\Gamma \,|\, \mu \vdash_{pc} \langle \textsc{Ref}\langle b\rangle, \textsc{Mut}\rangle x = e; s}$$

$$\textsc{VarDec}\quad \frac{x \notin Dom(\mu) \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell, \sigma\rangle \qquad \Gamma \,|\, \mu[x \mapsto \langle \textsc{Ref}\langle b\rangle, \textsc{FlowS}\langle \ell\rangle, \sigma\rangle] \vdash_{pc} s}{\Gamma \,|\, \mu \vdash_{pc} \langle \textsc{Ref}\langle b\rangle, \sigma\rangle x = e; s}$$

$$\textsc{ArrDec}\quad \frac{x \notin Dom(\mu) \qquad \Gamma \,|\, \mu \vdash e : \langle \textsc{Arr}\langle b, n\rangle, \ell, \sigma\rangle \qquad \Gamma \,|\, \mu[x \mapsto \langle \textsc{Arr}\langle b, n\rangle, \ell, \sigma\rangle] \vdash_{pc} s}{\Gamma \,|\, \mu \vdash_{pc} \langle \textsc{Arr}\langle b, n\rangle, \ell, \sigma\rangle x = e; s}$$

$$\textsc{VarAssign}\quad \frac{\mu(x) = \langle \textsc{Ref}\langle b\rangle, \ell, \textsc{Mut}\rangle \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell', \textsc{Const}\rangle \qquad \ell' \sqcup pc \sqsubseteq \ell \qquad \Gamma \,|\, \mu \vdash_{pc} s}{\Gamma \,|\, \mu \vdash_{pc} x := e; s}$$

$$\textsc{VarAssignFlowS}\quad \frac{\mu(x) = \langle \textsc{Ref}\langle b\rangle, \textsc{FlowS}\langle \ell\rangle, \textsc{Mut}\rangle \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell', \textsc{Const}\rangle \qquad \Gamma \,|\, \mu[x \mapsto \langle \textsc{Ref}\langle b\rangle, \textsc{FlowS}\langle \ell'\rangle\ \textsc{Mut}\rangle] \vdash_{pc} s}{\Gamma \,|\, \mu \vdash_{pc} x := e; s}$$

$$\textsc{ArrAssign}\quad \frac{\mu(x) = \langle \textsc{Arr}\langle b, n\rangle, \ell, \textsc{Mut}\rangle \qquad \Gamma \,|\, \mu \vdash e_1 : \langle \textsc{UInt}, \textsc{Public}, \textsc{Const}\rangle \qquad SMT(e_1 < n) \qquad \Gamma \,|\, \mu \vdash e_2 : \langle b, \ell', \textsc{Const}\rangle \qquad \ell' \sqcup pc \sqsubseteq \ell \qquad \Gamma \,|\, \mu \vdash_{pc} s}{\Gamma \,|\, \mu \vdash_{pc} x[e_1] := e_2; s}$$

$$\textsc{ArrAssignDyn}\quad \frac{\mu(x) = \langle \textsc{Arr}\langle b, x_n\rangle, \ell, \textsc{Mut}\rangle \qquad \Gamma \,|\, \mu \vdash e_1 : \langle \textsc{UInt}, \textsc{Public}, \textsc{Const}\rangle \qquad SMT(e_1 < x_n) \qquad \Gamma \,|\, \mu \vdash e_2 : \langle b, \ell', \textsc{Const}\rangle \qquad \ell' \sqcup pc \sqsubseteq \ell \qquad \Gamma \,|\, \mu \vdash_{pc} s}{\Gamma \,|\, \mu \vdash_{pc} x[e_1] := e_2; s}$$

$$\textsc{If}\quad \frac{\Gamma \,|\, \mu \vdash e : \langle \textsc{Bool}, \ell, \sigma\rangle \qquad pc' = \ell \sqcup pc \qquad \Gamma \,|\, \mu \vdash_{pc'} s_1 \qquad \Gamma \,|\, \mu \vdash_{pc'} s_2 \qquad \mu^* = extract\mu[\ell](s_1, s_2) \qquad pc^* = extractpc[pc'](s_1, s_2) \qquad \Gamma \,|\, \mu^* \vdash_{pc^*} s}{\Gamma \,|\, \mu \vdash_{pc} \textsc{if}\ e\ \{s_1\}\ \textsc{else}\ \{s_2\}; s}$$

$$\textsc{For}\quad \frac{\Gamma \,|\, \mu \vdash e_1 : \langle b, \textsc{Public}, \textsc{Const}\rangle \qquad \Gamma \,|\, \mu \vdash e_2 : \langle b, \textsc{Public}, \textsc{Const}\rangle \qquad b = \textsc{UInt}\ \text{ or }\ b = \textsc{Int} \qquad \text{typecheck } s_1 \text{ somehow???}}{\Gamma \,|\, \mu \vdash_{pc} \textsc{for}\ \langle b\rangle x\ \textsc{from}\ e_1\ \textsc{to}\ e_2\ \{s_1\}; s}$$

$$\textsc{Ret}\quad \frac{\mathbb{F}(f) = fdec : \langle b, \ell\rangle \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell'\rangle \qquad \ell' \sqcup pc \sqsubseteq \ell}{\Gamma \,|\, \mu \vdash_{pc} \textsc{return}\ e}$$

Interesting Semantics

$$\boxed{\begin{array}{l} \Sigma, \mu, s \longrightarrow \Sigma', \mu', s' \\ \Sigma, \mu, e \hookrightarrow \Sigma', \mu', e' \end{array}}$$

$$\textsc{Seq}\ \frac{\Sigma, \mu, s_1 \longrightarrow \Sigma', \mu', s_1'}{\Sigma, \mu, s_1; s_2 \longrightarrow \Sigma', \mu', s_1'; s_2} \qquad \textsc{Skip}\ \frac{}{\Sigma, \mu, \text{SKIP}; s_2 \longrightarrow \Sigma, \mu, s_2}$$

$$\textsc{Ret}\ \frac{}{\Sigma, \mu, \text{RETURN } v; s_2 \longrightarrow \Sigma, \mu, \text{RETURN } v} \qquad \textsc{VarDec}\ \frac{\Sigma' = \Sigma[x \mapsto r] \qquad \mu' = \mu[r \mapsto v] \qquad \text{fresh } r}{\Sigma, \mu, \langle \tau, \cdot, \sigma \rangle x = v \longrightarrow \Sigma', \mu', \text{SKIP}}$$

$$\textsc{VarAssign}\ \frac{\mu' = \mu[r \mapsto v]}{\Sigma, \mu, r := v \longrightarrow \Sigma, \mu', \text{SKIP}} \qquad \textsc{IfTrue}\ \frac{v = \text{TRUE}}{\Sigma, \mu, \text{IF } v\ \{s_1\}\ \text{ELSE}\ \{s_2\} \longrightarrow \Sigma, \mu, s_1}$$

$$\textsc{IfFalse}\ \frac{v = \text{FALSE}}{\Sigma, \mu, \text{IF } v\ \{s_1\}\ \text{ELSE}\ \{s_2\} \longrightarrow \Sigma, \mu, s_2}$$

$$\textsc{ForIter}\ \frac{v_1 < v_2 \qquad v_1' = v_1 + 1}{\Sigma, \mu, \text{FOR } \langle b \rangle x \text{ FROM } v_1 \text{ TO } v_2\ \{s\} \longrightarrow \Sigma, \mu, s[x \mapsto v_1]; \text{FOR } \langle b \rangle x \text{ FROM } v_1' \text{ TO } v_2\ \{s\}}$$

$$\textsc{ForEnd}\ \frac{v_1 \geq v_2}{\Sigma, \mu, \text{FOR } \langle b \rangle x \text{ FROM } v_1 \text{ TO } v_2\ \{s\} \longrightarrow \Sigma, \mu, \text{SKIP}} \qquad \textsc{Var}\ \frac{\Sigma(x) = r \qquad \mu(r) = v}{\Sigma, \mu, x \hookrightarrow \Sigma, \mu, v}$$

$$\textsc{Ref}\ \frac{\Sigma(x) = r}{\Sigma, \mu, \text{REF } x \hookrightarrow \Sigma, \mu, r}$$

$$\textsc{FnCall}\ \frac{\begin{array}{c} \mathbb{F}(f) = fdec\ f(x_1, \ldots, x_n)\ \{s\} \qquad \Sigma_0 = \{x_1 \mapsto r_1, \ldots, x_n \mapsto r_n\} \\ \text{fresh } r_i \text{ when necessary} \qquad \Sigma_0, \mu, s \longrightarrow^* \Sigma_0', \mu', \text{RETURN } v \qquad \mu'' = copyback(\mu, \mu') \end{array}}{\Sigma, \mu, f(v_1, \ldots, v_n) \hookrightarrow \Sigma, \mu'', v}$$