Grammar

Base type

b ::=

| $\textsc{Bool}$
| $\textsc{UInt}_n$
| $\textsc{Int}_n$

Type

τ ::=

| b
| $\textsc{Ref}\langle b\rangle$
| $\textsc{Arr}\langle b, n\rangle$
| $\textsc{Arr}\langle b, x\rangle$ — x must be $\langle \textsc{Ref}\langle \textsc{UInt}\rangle, \textsc{Public}, \textsc{Const}\rangle$

Label

ℓ ::=

| $\textsc{Public}$
| $\textsc{Secret}$

Variable label

ℓ^x ::=

| ℓ
| $\textsc{Float}\langle \ell\rangle$

Mutability

σ ::=

| $\textsc{Const}$
| $\textsc{Mut}$

Expression

e ::=

$\textsc{true}$	
$\textsc{false}$	
c	integer literal
x	variable
$x[e]$	array get
$\langle b, n, b_x\rangle x \Rightarrow e$	array comprehension
$\textsc{view}(x, e, n)$	array view
$\ominus e$	unary op
$e_1 \oplus e_2$	binary op
$e_1 \,?\, e_2 : e_3$	ternary op
$\textsc{ref}\ x$	mut ref
$f(e_1, \ldots, e_n)$	function call

Statement

s ::=

$s_1; s_2$	sequence
$\langle \textsc{Ref}\langle b\rangle, \sigma\rangle x = e$	variable declaration
$\langle \textsc{Arr}\langle b, n\rangle, \ell, \sigma\rangle x = e$	array declaration
$x := e$	variable assignment
$x[e_1] := e_2$	array assignment
$\textsc{if}\ e\ \{s_1\}\ \textsc{else}\ \{s_2\}$	conditional
$\textsc{for}\ \langle b\rangle x\ \textsc{from}\ e_1\ \textsc{to}\ e_2\ \{s\}$	loop
$\textsc{return}\ e$	return

Function Definition

$fdec$ ::=

| $\langle b, \ell\rangle f(\langle \tau_1, \ell_1, \sigma_1\rangle x_1, \ \ldots\ , \langle \tau_n, \ell_n, \sigma_n\rangle x_n)\ \{s\}$

Metavariables

Type context

$$\Gamma \;::=\; \emptyset \;\mid\; \Gamma[e \mapsto \langle \tau, \ell, \sigma \rangle]$$

Variable type store

$$\mu \;::=\; \emptyset \;\mid\; \mu[x \mapsto \langle \tau, \ell^x, \sigma \rangle]$$

Function type store

$$\mathbb{F} \;::=\; \emptyset \;\mid\; \mathbb{F}[f \mapsto fdec(\langle \tau_1, \ell_1, \sigma_1 \rangle, \ldots, \langle \tau_n, \ell_n, \sigma_n \rangle) : \langle b, \ell \rangle]$$

Type Lattice

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

$$\frac{}{\textsc{Mut} <_\sigma \textsc{Const}} \qquad \frac{\Gamma \mid \mu \vdash e : \langle b, \ell, \textsc{Const} \rangle \qquad b \leq_\tau b' \qquad \ell \leq_\ell \ell'}{\Gamma \mid \mu \vdash e : \langle b', \ell', \textsc{Const} \rangle}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Statements $\boxed{\langle \mu, \ell_s, r\rangle \vdash s \;\rightarrow\; \langle \mu', \ell_s', r'\rangle}$

$$\textsc{Seq}\quad \frac{\langle \mu, \ell_s, r\rangle \vdash s_1 \;\rightarrow\; \langle \mu', \ell_s', r'\rangle \qquad \langle \mu', \ell_s', r'\rangle \vdash s_2 \;\rightarrow\; \langle \mu'', \ell_s'', r''\rangle}{\langle \mu, \ell_s, r\rangle \vdash s_1; s_2 \;\rightarrow\; \langle \mu'', \ell_s'', r''\rangle}$$

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

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

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

$$\textsc{VarAssign}\quad \frac{\mu(x) = \langle \textsc{Ref}\langle b\rangle, \ell, \textsc{Mut}\rangle \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell', \textsc{Const}\rangle \qquad \ell_s \vee \ell' \leq_\ell \ell}{\langle \mu, \ell_s, r\rangle \vdash x := e \;\rightarrow\; \langle \mu, \ell_s, r\rangle}$$

$$\textsc{VarAssignFloat}\quad \frac{\mu(x) = \langle \textsc{Ref}\langle b\rangle, \textsc{Float}\langle \ell\rangle, \textsc{Mut}\rangle \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell', \textsc{Const}\rangle}{\langle \mu, \ell_s, r\rangle \vdash x := e \;\rightarrow\; \langle \mu[x \mapsto \langle \textsc{Ref}\langle b\rangle, \textsc{Float}\langle \ell'\rangle, \textsc{Mut}\rangle], \ell_s, r\rangle}$$

$$\textsc{ArrAssign}\quad \frac{\begin{array}{c}\mu(x) = \langle \textsc{Arr}\langle b, n\rangle, \ell, \textsc{Mut}\rangle \qquad \Gamma \,|\, \mu \vdash e_1 : \langle \textsc{UInt}, \textsc{Public}, \textsc{Const}\rangle \\ SMT(e_1 < n) \qquad \Gamma \,|\, \mu \vdash e_2 : \langle b, \ell', \textsc{Const}\rangle \qquad \ell_s \vee \ell' \leq_\ell \ell\end{array}}{\langle \mu, \ell_s, r\rangle \vdash x[e_1] := e_2 \;\rightarrow\; \langle \mu, \ell_s, r\rangle}$$

$$\textsc{ArrAssignDyn}\quad \frac{\begin{array}{c}\mu(x) = \langle \textsc{Arr}\langle b, x_n\rangle, \ell, \textsc{Mut}\rangle \qquad \Gamma \,|\, \mu \vdash e_1 : \langle \textsc{UInt}, \textsc{Public}, \textsc{Const}\rangle \\ SMT(e_1 < x_n) \qquad \Gamma \,|\, \mu \vdash e_2 : \langle b, \ell', \textsc{Const}\rangle \qquad \ell_s \vee \ell' \leq_\ell \ell\end{array}}{\langle \mu, \ell_s, r\rangle \vdash x[e_1] := e_2 \;\rightarrow\; \langle \mu, \ell_s, r\rangle}$$

$$\textsc{If}\quad \frac{\begin{array}{c}\Gamma \,|\, \mu \vdash e : \langle \textsc{Bool}, \ell, \sigma\rangle \\ \langle \mu, \ell_s, r\rangle \vdash s_1 \;\rightarrow\; \langle \mu', \ell_s', r'\rangle \qquad \langle \mu, \ell_s, r\rangle \vdash s_2 \;\rightarrow\; \langle \mu'', \ell_s'', r''\rangle \\ \mu^* = join\mu(\mu, \mu', \mu'', \ell) \qquad \ell_s^*, r^* = join\ell_s r(\ell_s, \ell_s', \ell_s'', r, r', r'')\end{array}}{\langle \mu, \ell_s, r\rangle \vdash \textsc{if}\ e\ \{s_1\}\ \textsc{else}\ \{s_2\} \;\rightarrow\; \langle \mu^*, \ell_s^*, r^*\rangle}$$

$$\textsc{For}\quad \frac{\begin{array}{c}\Gamma \,|\, \mu \vdash e_1 : \langle b, \textsc{Public}, \textsc{Const}\rangle \qquad \Gamma \,|\, \mu \vdash e_2 : \langle b, \textsc{Public}, \textsc{Const}\rangle \qquad b = \textsc{UInt}\ \text{or}\ b = \textsc{Int} \\ \langle \mu[x \mapsto \langle \textsc{Ref}\langle b\rangle, \textsc{Public}, \textsc{Const}\rangle], \ell_s, r\rangle \vdash s \;\rightarrow\; \langle \mu', \ell_s', r'\rangle \qquad \mu'' = scoping(\mu, \mu')\end{array}}{\langle \mu, \ell_s, r\rangle \vdash \textsc{for}\ \langle b\rangle x\ \textsc{from}\ e_1\ \textsc{to}\ e_2\ \{s\} \;\rightarrow\; \langle \mu'', \ell_s', r'\rangle}$$

$$\textsc{Ret}\quad \frac{\mathbb{F}(f) = fdec : \langle b, \ell_1\rangle \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell_2\rangle}{\langle \mu, \ell_s, r\rangle \vdash \textsc{return}\ e \;\rightarrow\; \langle \mu, \ell_s, \textsc{true}\rangle}$$

Interesting Semantics

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

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

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

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

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

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

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

$$\textsc{Ref}\ \frac{\Sigma(x) = r}{\Sigma, \mu, \text{REF } x \hookrightarrow \Sigma, \mu, r} \qquad \textsc{FnCall}\ \frac{\begin{array}{c}\mathbb{F}(f) = fdec\ f(x_1, \ldots, x_n)\ \{s\} \\ \Sigma_0 = \{x_1 \mapsto v_1, \ldots, x_n \mapsto v_n\} \qquad \Sigma_0, \mu, s \longrightarrow^* \Sigma_0', \mu', \text{RETURN } v\end{array}}{\Sigma, \mu, f(v_1, \ldots, v_n) \hookrightarrow \Sigma, \mu', v}$$