### Grammar

Base type

$$\begin{array}{lll} b & ::= & \\ & | & \textsc{Bool} \\ & | & \textsc{UInt}_n \\ & | & \textsc{Int}_n \end{array}$$

Type

$$\begin{array}{llll} \tau & ::= & & \\ & | & b & \\ & | & \textsc{Arr}\langle b, n\rangle & \\ & | & \textsc{Arr}\langle b, x\rangle & x \text{ must be } \langle \textsc{UInt}, \textsc{Public}, \textsc{Const}\rangle \end{array}$$

Label

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

Mutability

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

Expression

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

Statement

$$\begin{array}{llll} s & ::= & & \\ & | & s_1; s_2 & \text{sequence} \\ & | & \langle \tau, \sigma\rangle x := e & \text{variable declaration} \\ & | & x := e & \text{variable assignment} \\ & | & x[e_1] = e_2 & \text{array assignment} \\ & | & \textsc{if}\ e\ \{s_1\}\ \textsc{else}\ \{s_2\} & \text{conditional} \\ & | & \textsc{for}\ \langle b\rangle x\ \textsc{from}\ e_1\ \textsc{to}\ e_2\ \{s\} & \text{loop} \\ & | & \textsc{return}\ e & \text{return} \end{array}$$

Function Definition

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

### Metavariables

Type context

$$\begin{array}{lll} \Gamma & ::= & \\ & | & \emptyset \\ & | & \Gamma[e \mapsto \langle \tau, \ell, \sigma\rangle] \end{array}$$

Variable type store

$$\begin{array}{lll} \mu & ::= & \\ & | & \emptyset \\ & | & \mu[x \mapsto \langle \tau, \ell, \sigma\rangle] \end{array}$$

Function type store

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

### Type Lattice

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

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

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

## Expressions

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

$\textsc{Var}$

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

$\textsc{Unop}$

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

$\textsc{Binop}$

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

$\textsc{Ternop}$

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

$\textsc{ArrGet}$

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

$\textsc{ArrGetDyn}$

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

$\textsc{ArrComp}$

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

$\textsc{ArrView}$

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

$\textsc{ArrViewDyn}$

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

$\textsc{MutRef}$

$$\frac{\mu(x) = \langle \tau, \ell, \textsc{Mut} \rangle}{\Gamma \mid \mu \vdash \textsc{ref}\ x : \langle \tau, \ell, \textsc{Mut} \rangle}$$

$\textsc{FnCall}$

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

$\textsc{True}$

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

$\textsc{False}$

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

$\textsc{PosNumber}$

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

$\textsc{NegNumber}$

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

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

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

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

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

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

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

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

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

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

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