Grammar

Base type
b ::=
| Bool
| UInt_n
| Int_n

Type
τ ::=
| b
| $\mathrm{Arr}\langle b, n\rangle$

Label
ℓ ::=
| Public
| Secret

Expression
e ::=

|	true	
|	false	
|	c	integer literal
|	x	variable
|	$x[e]$	array get
|	$\langle\tau, n\rangle x \Rightarrow e$	array comprehension
|	$\mathrm{view}(x, e, n)$	array view
|	$\ominus e$	unary op
|	$e_1 \oplus e_2$	binary op
|	ref x	mut ref
|	$f(e_1, \ldots, e_n)$	function call

Mutability
σ ::=
| Const
| Mut

Statement
s ::=

|	$s_1; s_2$	sequence
|	$\langle\tau, \ell, \sigma\rangle x := e$	variable declaration
|	$x := e$	variable assignment
|	$x[e_1] = e_2$	array assignment
|	if e $\{s_1\}$ else $\{s_2\}$	conditional
|	for $\langle b\rangle x$ from e_1 to e_2 $\{s\}$	loop
|	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
Γ ::=
| $\emptyset$
| $\Gamma[e \mapsto \langle\tau, \ell, \sigma\rangle]$

Variable type store
μ ::=
| $\emptyset$
| $\mu[x \mapsto \langle\tau, \ell, \sigma\rangle]$

Function type store
$\mathbb{F}$ ::=
| $\emptyset$
| $\mathbb{F}[f \mapsto fdec(\langle\tau_1, \ell_1, \sigma_1\rangle, \ldots, \langle\tau_n, \ell_n, \sigma_n\rangle) : \langle\tau_f, \ell_f, \sigma_f\rangle]$

Type Lattice

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

$$\frac{}{\textsc{Mut} <_\sigma \textsc{Const}} \qquad \frac{\Gamma \,|\, \mu \vdash e : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \tau_1 \leq_\tau \tau_2 \qquad \ell_1 \leq_\ell \ell_2 \qquad \sigma_1 \leq_\sigma \sigma_2}{\Gamma \,|\, \mu \vdash e : \langle \tau_2, \ell_2, \sigma_2 \rangle} \qquad \frac{}{\ell \cup \ell = \ell}$$

$$\frac{}{\ell \cup \textsc{Secret} = \textsc{Secret}} \qquad \frac{}{\textsc{Secret} \cup \ell = \textsc{Secret}}$$

Expressions

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

$$\textsc{Var}\ \frac{\mu(x) = \langle \tau, \ell, \sigma \rangle}{\Gamma \,|\, \mu \vdash x : \langle \tau, \ell, \textsc{Const} \rangle} \qquad \textsc{Unop}\ \frac{\Gamma \,|\, \mu \vdash e : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \ominus : \langle \tau_1, \ell_1, \sigma_1 \rangle \to \langle \tau_2, \ell_2, \sigma_2 \rangle}{\Gamma \,|\, \mu \vdash \ominus e : \langle \tau_2, \ell_2, \sigma_2 \rangle}$$

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

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

$$\textsc{ArrComp}\ \frac{\Gamma \,|\, \mu[x \mapsto \langle b, \ell, \textsc{Const} \rangle] \vdash e : \langle b, \ell, \sigma \rangle}{\Gamma \,|\, \mu \vdash \langle b, n \rangle x \Rightarrow e : \langle \textsc{Arr}\langle b, n \rangle, \ell, \textsc{Mut} \rangle}$$

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

$$\textsc{MutRef}\ \frac{\mu(x) = \langle \tau, \ell, \textsc{Mut} \rangle}{\Gamma \,|\, \mu \vdash \textsc{ref}\ x : \langle \tau, \ell, \textsc{Mut} \rangle} \qquad \textsc{FnCall}\ \frac{\begin{array}{c}\mathbb{F}(f) = \mathit{fdec}(\langle \tau_1, \ell_1, \sigma_1 \rangle, \ldots, \langle \tau_n, \ell_n, \sigma_n \rangle) : \langle \tau_f, \ell_f, \sigma_f \rangle \\ \Gamma \,|\, \mu \vdash e_1 : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \ldots \qquad \Gamma \,|\, \mu \vdash e_n : \langle \tau_n, \ell_n, \sigma_n \rangle\end{array}}{\Gamma \,|\, \mu \vdash f(e_1, \ldots, e_n) : \langle \tau_f, \ell_f, \sigma_f \rangle}$$

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

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

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

Statements $\boxed{\langle \mu, \ell_s, r_? \rangle \vdash s \;\to\; \langle \mu', \ell'_s, r'_? \rangle}$

$$\textsc{Seq}\quad \frac{\Delta \vdash s_1 \;\to\; \Delta' \qquad \Delta' \vdash s_2 \;\to\; \Delta''}{\Delta \vdash s_1; s_2 \;\to\; \Delta''}$$

$$\textsc{VarDec}\quad \frac{x \notin \mathit{Dom}(\mu) \qquad \ell_s \leq_\ell \ell \qquad \Gamma \,|\, \mu \vdash e : \langle \tau, \ell, \sigma \rangle}{\langle \mu, \ell_s, r_? \rangle \vdash \langle \tau, \ell, \sigma \rangle x := e \;\to\; \langle \mu \mapsto x : \langle \tau, \ell, \sigma \rangle, \ell_s, r_? \rangle}$$

$$\textsc{VarDec*}\quad \frac{x \notin \mathit{Dom}(\mu) \qquad \ell_s \leq_\ell \ell \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell, \textsc{Const} \rangle}{\langle \mu, \ell_s, r_? \rangle \vdash \langle b, \ell, \textsc{Mut} \rangle x := e \;\to\; \langle \mu \mapsto x : \langle b, \ell, \textsc{Mut} \rangle, \ell_s, r_? \rangle}$$

$$\textsc{VarAssign}\quad \frac{\mu(x) = \langle b, \ell, \textsc{Mut} \rangle \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell, \textsc{Const} \rangle}{\Delta\langle \ell_s \rangle \vdash x := e : \textsc{Public}}$$

$$\textsc{ArrAssign}\quad \frac{\mu(a) = \langle \textsc{Arr}\langle b, n \rangle, \ell_1, \textsc{Mut} \rangle \qquad \Gamma \vdash e_1 : \langle \textsc{UInt}_{max}, \textsc{Public} \rangle \qquad \Gamma \vdash e_2 : \langle b, \ell_2 \rangle \qquad \ell_2 \leq_\ell \ell_1}{\Delta\langle \ell_s \rangle \vdash a[e_1] := e_2 : \textsc{Public}}$$

$$\textsc{If}\quad \frac{\Gamma \vdash e : \langle \textsc{Bool}, \ell \rangle \qquad \Delta\langle \ell \cup \ell_s \rangle \vdash s_1 : \ell'_s \qquad \Delta\langle \ell \cup \ell_s \rangle \vdash s_2 : \ell''_s}{\Delta\langle \ell_s \rangle \vdash \textsc{if}\ e\ \{s_1\}\ \textsc{else}\ \{s_2\} : \ell'_s \cup \ell''_s}$$

$$\textsc{For}\quad \frac{\Gamma \vdash e_1 : \langle b, \textsc{Public} \rangle \qquad \Gamma \vdash e_2 : \langle b, \textsc{Public} \rangle \qquad b = \textsc{UInt}_s \vee b = \textsc{Int}_s \qquad \Delta\langle \ell_s \rangle \vdash s : \ell'_s}{\begin{array}{c}\Delta\langle \ell_s \rangle \vdash \textsc{for}\ \langle b \rangle x\ \textsc{from}\ e_1\ \textsc{to}\ e_2\ \{s\} : \ell'_s \\ \mu(x) = \langle b, \textsc{Public}, \textsc{Const} \rangle \text{ (scoping?)}\end{array}}$$

$$\textsc{Ret}\quad \frac{\Gamma \vdash e : \langle b, \ell_1 \rangle \qquad \mathbb{F}(f) = \mathit{fdec} : \langle b, \ell_2 \rangle \qquad \ell_1 \leq_\ell \ell_2}{\Delta\langle \ell_s \rangle \vdash \textsc{return}\ e : \ell_s}$$