Types

Integer type
$$\begin{array}{lll} I & ::= & \\ & \mid & \textsc{UInt}_n \\ & \mid & \textsc{Int}_n \end{array}$$

Base type
$$\begin{array}{lll} \beta & ::= & \\ & \mid & I \\ & \mid & \textsc{Bool} \end{array}$$

Ref type
$$\begin{array}{lll} \rho & ::= & \\ & \mid & \textsc{Ref}[\beta] \end{array}$$

Array type
$$\begin{array}{lll} \alpha & ::= & \\ & \mid & \textsc{Arr}[\beta, \underline{e}] \end{array}$$

Expression Type
$$\begin{array}{lll} \eta & ::= & \\ & \mid & \beta_\ell \\ & \mid & \alpha_\ell^m \end{array}$$

Variable Type
$$\begin{array}{lll} \tau & ::= & \\ & \mid & \rho_\ell^m \\ & \mid & \alpha_\ell^m \end{array}$$

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

Mutability
$$\begin{array}{lll} m & ::= & \\ & \mid & \textsc{Const} \\ & \mid & \textsc{Mut} \end{array}$$

Metavariables

Type context
$$\begin{array}{lll} \Gamma & ::= & \\ & \mid & \emptyset \\ & \mid & \Gamma[\text{æ} \mapsto \eta] \\ & \mid & \Gamma[x \mapsto \tau] \end{array}$$

Function type store
$$\begin{array}{lll} \mathbb{F} & ::= & \\ & \mid & \emptyset \\ & \mid & \mathbb{F}[f \mapsto \prod_{i=1}^{n} \tau_i \to \beta_\ell] \end{array}$$

Type Lattice

No implicit casts between any integer types; explicit casting only.

$$\frac{}{\textsc{Public} \sqsubset \textsc{Secret}} \qquad \frac{\beta_1 \sqsubseteq \beta_2 \qquad \ell_1 \sqsubseteq \ell_2}{\beta_{\ell_1} \sqsubseteq \beta_{\ell_2}} \qquad \frac{\ell_1 \sqsubseteq \ell_2}{\alpha_{\ell_1}^m \sqsubseteq \alpha_{\ell_2}^{\textsc{Const}}} \qquad \frac{\Gamma \vdash \text{æ} : \eta_1 \qquad \tau_1 \sqsubset \eta_2}{\Gamma \vdash \text{æ} : \eta_2}$$

$$\frac{\Gamma \vdash a : \textsc{Arr}\big[\beta, \underline{e_1}\big]_\ell^m \qquad \mathrm{SMT}(e_1 = e_2)}{\Gamma \vdash a : \textsc{Arr}\big[\beta, \underline{e_2}\big]_\ell^m}$$

Parameter Passing

$$\frac{\Gamma \vdash e : \beta_\ell}{\textsc{canpass}\ \textsc{Ref}[\beta]_\ell^{\textsc{Const}} \leftarrow e} \qquad \frac{\Gamma \vdash a : \alpha_\ell^{\textsc{Const}}}{\textsc{canpass}\ \alpha_\ell^{\textsc{Const}} \leftarrow a} \qquad \frac{\Gamma(x) = \rho_\ell^{\textsc{Mut}}}{\textsc{canpass}\ \rho_\ell^{\textsc{Mut}} \leftarrow \textsc{ref}\ x}$$

$$\frac{\Gamma(x) = \alpha_\ell^{\textsc{Mut}}}{\textsc{canpass}\ \alpha_\ell^{\textsc{Mut}} \leftarrow \textsc{ref}\ x}$$

Grammar

EXPRESSION

e	$::=$		
	$\mid$	TRUE	
	$\mid$	FALSE	
	$\mid$	$\underline{c}$	integer literal
	$\mid$	$\underline{x}$	variable
	$\mid$	$x[e]$	array get
	$\mid$	$\underline{\text{LEN } x}$	array length
	$\mid$	$(I)e$	int cast
	$\mid$	$\ominus e$	unary op
	$\mid$	$e_1 \oplus e_2$	binary op
	$\mid$	$e_1 \,?\, e_2 : e_3$	ternary op
	$\mid$	$f(arg_1, \ldots, arg_n)$	function call
	$\mid$	DECLASSIFY e	declassify

ARRAY EXPRESSION

a	$::=$		
	$\mid$	x	variable
	$\mid$	ZEROS $\underline{e}$	zero array
	$\mid$	COPY x	array copy
	$\mid$	VIEW $x, e_1, \underline{e'}$	array view
	$\mid$	ARRCOMP$[\beta, \underline{e}]$ $x \Rightarrow e$	array comprehension

ARGUMENT

arg	$::=$		
	$\mid$	e	expression (by value)
	$\mid$	a	array (by const ref)
	$\mid$	REF x	variable (by mut ref)

STATEMENT

s	$::=$		
	$\mid$	$\diamond$	empty
	$\mid$	SKIP	skip
	$\mid$	$s_1; s_2$	sequence
	$\mid$	LET x@$\tau = æ$	variable declaration
	$\mid$	$x := e$	variable assignment
	$\mid$	$x[e_1] := e_2$	array assignment
	$\mid$	IF e THEN s_1 ELSE s_2	conditional
	$\mid$	FOR x@I FROM e_1 TO e_2 DO s	loop
	$\mid$	RETURN e	return

FUNCTION DEFINITION

$fdec$	$::=$	
	$\mid$	FDEC $f(x$@$\tau_1, \cdots, x$@$\tau_n) : \beta_\ell \; \{s\}$

Expressions $\boxed{\Gamma \vdash e : \eta}$

$$\textsc{True}\quad \frac{}{\Gamma \vdash \textsc{true} : \textsc{Bool}_{\textsc{Public}}}$$

$$\textsc{False}\quad \frac{}{\Gamma \vdash \textsc{false} : \textsc{Bool}_{\textsc{Public}}}$$

$$\textsc{PosNumber}\quad \frac{c >= 0 \qquad n = \lceil \log_2 c \rceil}{\Gamma \vdash c : \textsc{UInt}_{n\textsc{Public}}}$$

$$\textsc{NegNumber}\quad \frac{c < 0 \qquad n = \lceil \log_2 |c| \rceil + 1}{\Gamma \vdash c : \textsc{Int}_{n\textsc{Public}}}$$

$$\textsc{Var}\quad \frac{\Gamma(x) = \rho_\ell^m}{\Gamma \vdash x : \beta_\ell}$$

$$\textsc{ArrVar}\quad \frac{\Gamma(x) = \alpha_\ell^m}{\Gamma \vdash x : \alpha_\ell^{\textsc{Const}}}$$

$$\textsc{IntCast}\quad \frac{\Gamma \vdash e : I_\ell}{\Gamma \vdash (I')e : I'_\ell}$$

$$\textsc{Unop}\quad \frac{\Gamma \vdash e : \eta_1 \qquad \ominus : \eta_1 \to \eta_2}{\Gamma \vdash \ominus e : \eta_2}$$

$$\textsc{Binop}\quad \frac{\Gamma \vdash e_1 : \eta_1 \qquad \Gamma \vdash e_2 : \eta_2 \qquad \oplus : \eta_1 \to \eta_2 \to \eta_3}{\Gamma \vdash e_1 \oplus e_2 : \eta_3}$$

$$\textsc{Ternop}\quad \frac{\Gamma \vdash e_1 : \eta_1 \qquad \Gamma \vdash e_2 : \eta_2 \qquad \Gamma \vdash e_3 : \eta_3 \qquad (\mathbf{?}\,\mathbf{:}) : \eta_1 \to \eta_2 \to \eta_3 \to \eta_4}{\Gamma \vdash e_1 \,\mathbf{?}\, e_2 \,\mathbf{:}\, e_3 : \eta_4}$$

$$\textsc{ArrGet}\quad \frac{\Gamma(x) = \textsc{Arr}\big[\beta, \underline{e_a}\big]_\ell^m \qquad \Gamma \vdash e : I_{\textsc{Public}} \qquad \mathrm{SMT}(0 \leq e < e_a)}{\Gamma \vdash x[e] : \beta_\ell}$$

$$\textsc{ArrLen}\quad \frac{\Gamma(x) = \textsc{Arr}\big[\beta, \underline{e_a}\big]_\ell^m \qquad \Gamma \vdash e_a : I_{\textsc{Public}}}{\Gamma \vdash \textsc{len}\ x : I_{\textsc{Public}}}$$

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

$$\textsc{ArrCopy}\quad \frac{\Gamma \vdash a : \textsc{Arr}[\beta, \underline{e}]_\ell^m}{\Gamma \vdash \textsc{copy}\ a : \textsc{Arr}[\beta, \underline{e}]_\ell^{\textsc{Mut}}}$$

$$\textsc{ArrView}\quad \frac{\Gamma \vdash a : \textsc{Arr}[\beta, \underline{e}]_\ell^m \qquad \mathrm{SMT}(0 \leq e_1 \leq e_1 + e' \leq e)}{\Gamma \vdash \textsc{view}\ x, e_1, \underline{e'} : \textsc{Arr}\big[\beta, \underline{e'}\big]_\ell^m}$$

$$\textsc{ArrComp}\quad \frac{\textsc{UInt}_{\lceil \log_2 e_a \rceil} \sqsubseteq I \qquad \Gamma[x \mapsto I_{\textsc{Public}}^{\textsc{Const}}] \vdash e : \beta_\ell}{\Gamma \mid \mu \vdash \textsc{arrcomp}[\beta, \underline{e_a}]\ x \Rightarrow e : \textsc{Arr}\big[\beta, \underline{e_a}\big]_\ell^{\textsc{Mut}}}$$

$$\textsc{FnCall}\quad \frac{\Gamma(f) = \prod_{i=1}^{n} \tau_i \to \beta_\ell \qquad \bigwedge_{i=1}^{n} \textsc{canpass}\ \tau_i \leftarrow \mathit{arg}_i}{\Gamma \vdash f(\mathit{arg}_1, \ldots, \mathit{arg}_n) : \beta_\ell}$$

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

$$\textsc{Empty}\quad \frac{}{\Gamma \vdash^{rp}_{pc} \diamond : rp}$$

$$\textsc{Skip}\quad \frac{\Gamma \vdash^{rp}_{pc} s : rp'}{\Gamma \vdash^{rp}_{pc} \text{SKIP}; s : rp'}$$

$$\textsc{VarDec}\quad \frac{x \notin Dom(\Gamma) \qquad \Gamma \vdash e : \beta_\ell \qquad \Gamma[x \mapsto \textsc{Ref}[\beta]^m_\ell] \vdash^{rp}_{pc} s : rp'}{\Gamma \vdash^{rp}_{pc} \text{LET } x@\textsc{Ref}[\beta]^m_\ell = e; s : rp'}$$

$$\textsc{ArrDec}\quad \frac{x \notin Dom(\Gamma) \qquad \Gamma \vdash a : \alpha^m_\ell \qquad \Gamma[x \mapsto \alpha^m_\ell] \vdash^{rp}_{pc} s : rp'}{\Gamma \vdash^{rp}_{pc} x@\alpha^m_\ell = a; s : rp'}$$

$$\textsc{VarAssign}\quad \frac{\Gamma(x) = \textsc{Ref}[\beta]^{\textsc{Mut}}_\ell \qquad \Gamma \vdash e : \beta_\ell \qquad rp \sqcup pc \sqsubseteq \ell \qquad \Gamma \vdash^{rp}_{pc} s : rp'}{\Gamma \vdash^{rp}_{pc} x := e; s : rp'}$$

$$\textsc{ArrAssign}\quad \frac{\Gamma(x) = \textsc{Arr}\big[\beta, e_a\big]^{\textsc{Mut}}_\ell \qquad \Gamma \vdash e_1 : I_{\textsc{Public}} \qquad \text{SMT}(0 \le e_1 < e_a) \qquad \Gamma \vdash e_2 : \beta_\ell \qquad rp \sqcup pc \sqsubseteq \ell \qquad \Gamma \vdash^{rp}_{pc} s : rp'}{\Gamma \mid \mu \vdash^{rp}_{pc} x[e_1] := e_2; s : rp'}$$

$$\textsc{If}\quad \frac{\Gamma \vdash e : \textsc{Bool}_\ell \qquad pc' = \ell \sqcup pc \qquad \Gamma \vdash^{rp}_{pc'} s_1 : rp_1 \qquad \Gamma \vdash^{rp}_{pc'} s_2 : rp_2 \qquad rp^* = rp_1 \sqcup rp_2 \qquad \Gamma \vdash^{rp^*}_{pc} s : rp'}{\Gamma \vdash^{rp}_{pc} \text{IF } e \text{ THEN } s_1 \text{ ELSE } s_2; s : rp'}$$

$$\textsc{For}\quad \frac{\Gamma \vdash e_1 : I_{\textsc{Public}} \qquad \Gamma \vdash e_2 : I_{\textsc{Public}} \qquad \Gamma[x \mapsto I_{\textsc{Public}}] \vdash^{rp}_{pc} s_1 : rp'}{\Gamma \mid \mu \vdash_{pc} \text{FOR } x@I \text{ FROM } e_1 \text{ TO } e_2 \text{ DO } s_1; s : rp'}$$

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

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

Interesting Semantics

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

$$\textsc{Seq}\ \frac{\Sigma, \mu, s_1 \longrightarrow \Sigma', \mu', s_1'}{\Sigma, \mu, s_1; s_2 \longrightarrow \Sigma', \mu', s_1'; s_2}$$

$$\textsc{Skip}\ \frac{}{\Sigma, \mu, \text{SKIP}; s_2 \longrightarrow \Sigma, \mu, s_2}$$

$$\textsc{Ret}\ \frac{}{\Sigma, \mu, \text{RETURN } v; s_2 \longrightarrow \Sigma, \mu, \text{RETURN } v}$$

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

$$\textsc{VarAssign}\ \frac{\mu' = \mu[r \mapsto v]}{\Sigma, \mu, r := v \longrightarrow \Sigma, \mu', \text{SKIP}}$$

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

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

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

$$\textsc{ForEnd}\ \frac{v_1 \geq v_2}{\Sigma, \mu, \text{FOR } \langle \beta \rangle x \text{ FROM } v_1 \text{ TO } v_2\ \{s\} \longrightarrow \Sigma, \mu, \text{SKIP}}$$

$$\textsc{Var}\ \frac{\Sigma(x) = r \qquad \mu(r) = v}{\Sigma, \mu, x \hookrightarrow \Sigma, \mu, v}$$

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

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