Types

$$
\begin{array}{lll}
\textsc{Base type} & \textsc{Label} & \textsc{Mutability} \\
\tau \quad ::= & \ell \quad ::= & \sigma \quad ::= \\
\quad \mid \quad \textsc{Bool} & \quad \mid \quad \textsc{Public} & \quad \mid \quad \textsc{Const} \\
\quad \mid \quad \textsc{UInt}\langle n\rangle & \quad \mid \quad \textsc{Secret} & \quad \mid \quad \textsc{Mut} \\
\quad \mid \quad \textsc{Int}\langle n\rangle & & \\
\quad \mid \quad \textsc{Arr}\langle \tau, n\rangle & &
\end{array}
$$

Type Lattice

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

$$\frac{}{\textsc{UInt}\langle n\rangle <_\tau \textsc{Int}\langle 2n\rangle} \qquad \frac{\tau_1 <_\tau \tau_2 \qquad \Gamma \vdash e : \langle \tau_1, \ell\rangle}{\Gamma \vdash e : \langle \tau_2, \ell\rangle} \qquad \frac{\ell_1 \leq_\ell \ell_2}{\ell_1 \cup \ell_2 = \ell_2}$$

$$\frac{\tau_1 <_\tau \tau_2 \qquad \Gamma \vdash e : \langle \textsc{Arr}\langle \tau_1, n\rangle, \ell\rangle}{\Gamma \vdash e : \langle \textsc{Arr}\langle \tau_2, n\rangle, \ell\rangle}$$

ArrSlice

$$\frac{\mu(a) = \langle \textsc{Arr}\langle \tau, n\rangle, \ell, \sigma\rangle \qquad \Gamma \vdash e : \langle \textsc{UInt}\langle max\rangle, \textsc{Public}\rangle \qquad n' \leq n}{\mu(a[e : n']) : \langle \textsc{Arr}\langle \tau, n'\rangle, \ell, \sigma\rangle}$$

Parameter Passing

$$\frac{\Gamma \vdash e : \langle \tau, \ell_1\rangle \qquad \ell_1 \leq_\ell \ell_2}{\langle \tau, \ell_2, \textsc{Const}\rangle \leftarrow e} \qquad \frac{\mu(x) = \langle \tau, \ell, \textsc{Mut}\rangle}{\langle \tau, \ell, \textsc{Mut}\rangle \leftarrow \textsc{Mut}\ x}$$

Expressions

Var

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

Unop

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

Binop

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

ArrGet

$$\frac{\mu(a) = \langle \textsc{Arr}\langle \tau, n\rangle, \ell, \sigma\rangle \qquad \Gamma \vdash e : \langle \textsc{UInt}\langle max\rangle, \textsc{Public}\rangle}{\Gamma \vdash a[e] : \langle \tau, \ell\rangle}$$

FnCall

$$\frac{\mathbb{F}(f) = fdec(p_1, \ldots, p_n) : \langle \tau, \ell\rangle \qquad p_1 \leftarrow v_1 \qquad \cdots \qquad p_n \leftarrow v_n}{\Gamma \vdash f(v_1, \ldots, v_n) : \langle \tau, \ell\rangle}$$

True

$$\frac{}{\Gamma \vdash true : \langle bool, \textsc{Public}\rangle}$$

False

$$\frac{}{\Gamma \vdash false : \langle bool, \textsc{Public}\rangle}$$

PosNumber

$$\frac{k >= 0 \qquad n = \lceil \log_2 k \rceil}{\Gamma \vdash k : \langle \textsc{UInt}\langle n\rangle, \textsc{Public}\rangle}$$

NegNumber

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

Statements

$$\textsc{Seq}\qquad \frac{\Sigma\langle\ell_s\rangle \vdash s_1 : \ell_s' \qquad \Sigma\langle\ell_s'\rangle \vdash s_2 : \ell_s''}{\Sigma\langle\ell_s\rangle \vdash s_1; s_2 : \ell_s' \cup \ell_s''}$$

$$\textsc{VarDec}\qquad \frac{\Gamma \vdash e : \langle\tau, \ell_1\rangle \qquad \ell_1 \leq_\ell \ell_2}{\begin{array}{c}\Sigma\langle\ell_s\rangle \vdash \langle\tau, \ell_2, \sigma\rangle x := e : \textsc{Public} \\ \mu(x) = \langle\tau, \ell_2, \sigma\rangle \text{ (scoping?)}\end{array}}$$

$$\textsc{VarAssign}\qquad \frac{\mu(x) = \langle\tau, \ell_1, \textsc{Mut}\rangle \qquad \Gamma \vdash e : \langle\tau, \ell_2\rangle \qquad \ell_2 \leq_\ell \ell_1}{\Sigma\langle\ell_s\rangle \vdash x := e : \textsc{Public}}$$

$$\textsc{ArrAssign}\qquad \frac{\mu(a) = \langle\textsc{Arr}\langle\tau, n\rangle, \ell_1, \textsc{Mut}\rangle \qquad \Gamma \vdash e_1 : \langle\text{UI}\textsc{nt}\langle max\rangle, \textsc{Public}\rangle \qquad \Gamma \vdash e_2 : \langle\tau, \ell_2\rangle \qquad \ell_2 \leq_\ell \ell_1}{\Sigma\langle\ell_s\rangle \vdash a[e_1] := e_2 : \textsc{Public}}$$

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

$$\textsc{For}\qquad \frac{\Gamma \vdash e_1 : \langle\tau, \textsc{Public}\rangle \qquad \Gamma \vdash e_2 : \langle\tau, \textsc{Public}\rangle \qquad \tau = \text{UI}\textsc{nt}\langle s\rangle \lor \tau = \textsc{Int}\langle s\rangle \qquad \Sigma\langle\ell_s\rangle \vdash s : \ell_s'}{\begin{array}{c}\Sigma\langle\ell_s\rangle \vdash \textsc{for}\ \langle\tau\rangle x\ \textsc{from}\ e_1\ \textsc{to}\ e_2\ \{s\} : \ell_s' \\ \mu(x) = \langle\tau, \textsc{Public}, \textsc{Const}\rangle \text{ (scoping?)}\end{array}}$$

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