Type Lattice

$$\frac{s_1 < s_2}{uint\langle s_1\rangle <_\tau uint\langle s_2\rangle} \qquad \frac{s_1 < s_2}{int\langle s_1\rangle <_\tau int\langle s_2\rangle} \qquad \frac{}{uint\langle s\rangle <_\tau int\langle 2s\rangle}$$

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

Expressions

$$\textsc{Var}\quad \frac{\mu(x) = \langle \tau, \ell, k \rangle \qquad k \neq \textsc{Arr}\langle s \rangle}{\Gamma \vdash x : \langle \tau, \ell \rangle}$$

$$\textsc{Unop}\quad \frac{\Gamma \vdash e : \langle \tau, \ell \rangle \qquad \ominus : \tau \to \tau}{\Gamma \vdash \ominus e : \langle \tau, \ell \rangle}$$

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

$$\textsc{ArrGet}\quad \frac{\mu(a) = \langle \tau, \ell, \textsc{Arr}\langle s \rangle \rangle \qquad \Gamma \vdash e : \mathit{uint}\langle \mathit{max} \rangle_{\textsc{Public}}}{\Gamma \vdash a[e] : \langle \tau, \ell \rangle}$$

$$\textsc{ValPass}\quad \frac{p : \langle \tau, \ell_1, \textsc{Val} \rangle \qquad \Gamma \vdash e : \langle \tau, \ell_2 \rangle \qquad \ell_2 \leq_\ell \ell_1}{p \leftarrow e}$$

$$\textsc{RefPassSecret}\quad \frac{p : \langle \tau, \textsc{Secret}, \textsc{Ref} \rangle \qquad \mu(x) = \langle \tau, \ell, k \rangle \qquad k \neq \textsc{Arr}\langle s \rangle}{p \leftarrow x}$$

$$\textsc{RefPassPublic}\quad \frac{p : \langle \tau, \textsc{Public}, \textsc{Ref} \rangle \qquad \mu(x) = \langle \tau, \textsc{Public}, k \rangle \qquad k \neq \textsc{Arr}\langle s \rangle}{p \leftarrow x}$$

$$\textsc{ArrPassSecret}\quad \frac{p : \langle \tau, \textsc{Secret}, \textsc{Arr}\langle s \rangle \rangle \qquad \mu(a) = \langle \tau, \ell, \textsc{Arr}\langle s \rangle \rangle}{p \leftarrow a}$$

$$\textsc{ArrPassPublic}\quad \frac{p : \langle \tau, \textsc{Public}, \textsc{Arr}\langle s \rangle \rangle \qquad \mu(a) = \langle \tau, \textsc{Public}, \textsc{Arr}\langle s \rangle \rangle}{p \leftarrow a}$$

$$\textsc{ArrPassSecretSlice}\quad \frac{p : \langle \tau, \textsc{Secret}, \textsc{Arr}\langle s_1 \rangle \rangle \qquad \mu(a) = \langle \tau, \ell, \textsc{Arr}\langle s_2 \rangle \rangle \qquad s_1 \leq s_2}{p \leftarrow a[n : n + s_1]}$$

$$\textsc{ArrPassPublicSlice}\quad \frac{p : \langle \tau, \textsc{Public}, \textsc{Arr}\langle s_1 \rangle \rangle \qquad \mu(a) = \langle \tau, \textsc{Public}, \textsc{Arr}\langle s_2 \rangle \rangle \qquad s_1 \leq s_2}{p \leftarrow a[n : n + s_1]}$$

$$\textsc{FnCall}\quad \frac{\mathbb{F}(f) = \mathit{fdec}(p_1 : \langle \tau_1, \ell_1, k_1 \rangle, \ldots, p_n : \langle \tau_n, \ell_n, k_n \rangle) : \langle \tau_r, \ell_r \rangle \qquad p_1 \leftarrow v_1 \qquad \cdots \qquad p_n \leftarrow v_n}{\Gamma \vdash f(v_1, \ldots, v_n) : \langle \tau_r, \ell_r \rangle}$$

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

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

Array literals are not expressions since they can only be used with ArrDec.

$$\textsc{PosNumber}\quad \frac{n >= 0 \qquad s = \lceil \log_2 n \rceil}{\Gamma \vdash n : \langle \mathit{uint}\langle s \rangle, \textsc{Public} \rangle}$$

$$\textsc{NegNumber}\quad \frac{n < 0 \qquad s = \lceil \log_2 |n| \rceil + 1}{\Gamma \vdash n : \langle \mathit{int}\langle s \rangle, \textsc{Public} \rangle}$$

Statements

$$\langle\tau,\ell_x\rangle x := e \implies \frac{x \notin \mu \qquad \Gamma \vdash e : \langle \tau, \ell_e\rangle \qquad \ell_e \leq_\ell \ell_x}{\mu(x) := \langle \tau, \ell_x, \textsc{Val}\rangle \qquad \mathcal{M}(x) := e}$$

$$\langle\tau,\ell_a\rangle a[s] := \textsc{ArrayInitializer} \implies \frac{a \notin \mu \qquad \textsc{ArrayInitializer} : \langle \tau, \ell_e\rangle \qquad \ell_e \leq_\ell \ell_a}{\mu(a) := \langle \tau, \ell_a, \textsc{Arr}\langle s\rangle\rangle \qquad \mathcal{M}(a) := \textsc{ArrayInitializer}}$$

$$x := e \implies \frac{\mu(x) = \langle \tau, \ell_x, k\rangle \qquad k \neq \textsc{Arr}\langle s\rangle \qquad \Gamma \vdash e : \langle \tau, \ell_e\rangle \qquad \ell_e \leq_\ell \ell_x}{\mathcal{M}(x) := e}$$

$$a[e_1] := e_2 \implies \frac{\mu(a) = \langle \tau, \ell_x, k\rangle \qquad k = \textsc{Arr}\langle s\rangle \qquad \Gamma \vdash e_1 : \langle \mathit{uint}\langle \mathit{max}\rangle, \textsc{Public}\rangle \qquad \Gamma \vdash e_2 : \langle \tau, \ell_e\rangle \qquad \ell_e \leq_\ell \ell_x}{\mathcal{M}(a, e_1) := e_2}$$

$$\text{if } (e)\{s_1\} \text{ else } \{s_2\} \implies \frac{\Gamma \vdash e : \langle \mathit{bool}, \ell\rangle}{}$$

$$\text{for } (\langle \tau, \textsc{Public}\rangle i \text{ from } e_1 \text{ to } e_2)\{s\} \implies \frac{i \notin \mu \qquad \Gamma \vdash e_1 : \langle \tau, \textsc{Public}\rangle \qquad \Gamma \vdash e_2 : \langle \tau, \textsc{Public}\rangle}{}$$

$$\text{return } e \implies \frac{\Gamma \vdash e : \langle \tau, \ell_e\rangle \qquad \mathbb{F}(f) = \mathit{fdec} : \langle \tau, \ell_f\rangle \qquad \ell_e \leq_\ell \ell_f}{}$$