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

Var

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

Unop

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

Binop

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

ArrGet

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

ValPass

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

RefPassSecret

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

RefPassPublic

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

ArrPassSecret

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

ArrPassPublic

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

FnCall

$$\frac{\mathbb{F}(f) = fdec(x_1 : \langle \tau_1, \ell_1, k_1\rangle, \ldots, x_n : \langle \tau_n, \ell_n, k_n\rangle) : \langle \tau_r, \ell_r\rangle \qquad x_1 \leftarrow v_1 \qquad \cdots \qquad x_n \leftarrow v_n}{\Gamma \vdash f(v_1, \ldots, v_n) : \langle \tau_r, \ell_r\rangle}$$

True

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

False

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

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

PosNumber

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

NegNumber

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