Types

Base Type τ			Label ℓ		Storage Type σ		
Bool	UInt$\langle s\rangle$	Int$\langle s\rangle$	Public	Secret	Val	Ref	Arr$\langle s\rangle$

Type Lattice

$$\frac{s_1 < s_2}{\textsc{UInt}\langle s_1\rangle <_\tau \textsc{UInt}\langle s_2\rangle} \qquad \frac{s_1 < s_2}{\textsc{Int}\langle s_1\rangle <_\tau \textsc{Int}\langle s_2\rangle} \qquad \frac{}{\textsc{UInt}\langle s\rangle <_\tau \textsc{Int}\langle 2s\rangle}$$

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

Parameter Passing

$$\frac{\Gamma \vdash e : \langle \tau, \ell_1\rangle \qquad \ell_1 \leq_\ell \ell_2}{\langle \tau, \ell_2, \textsc{Val}\rangle \leftarrow \textsc{Val}\ e} \qquad \frac{\mu(x) = \langle \tau, \ell, \sigma\rangle \qquad \sigma \neq \textsc{Arr}\langle s\rangle}{\langle \tau, \ell, \textsc{Ref}\rangle \leftarrow \textsc{Ref}\ x} \qquad \frac{\mu(a) = \langle \tau, \ell, \textsc{Arr}\langle s\rangle\rangle}{\langle \tau, \ell, \textsc{Arr}\langle s\rangle\rangle \leftarrow \textsc{Arr}\ a}$$

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

Expressions

$$\textsc{Var}\ \frac{\mu(x) = \langle \tau, \ell, \sigma\rangle \qquad \sigma \neq \textsc{Arr}\langle s\rangle}{\Gamma \vdash x : \langle \tau, \ell\rangle} \qquad \textsc{Unop}\ \frac{\Gamma \vdash e : \langle \tau_1, \ell\rangle \qquad \ominus : \tau_1 \rightarrow \tau_2}{\Gamma \vdash \ominus e : \langle \tau_2, \ell\rangle}$$

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

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

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

$$\textsc{False}\ \frac{}{\Gamma \vdash false : \langle bool, \textsc{Public}\rangle} \qquad \textsc{PosNumber}\ \frac{n >= 0 \qquad s = \lceil \log_2 n \rceil}{\Gamma \vdash n : \langle \textsc{UInt}\langle s\rangle, \textsc{Public}\rangle} \qquad \textsc{NegNumber}\ \frac{n < 0 \qquad s = \lceil \log_2 |n| \rceil + 1}{\Gamma \vdash n : \langle \textsc{Int}\langle s\rangle, \textsc{Public}\rangle}$$

Statements

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

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

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

$$\frac{\begin{array}{l}a[e_1] := e_2 \implies \\ \mu(a) = \langle \tau, \ell_x, \sigma \rangle \\ \sigma = \textsc{Arr}\langle s \rangle \qquad \Gamma \vdash e_1 : \langle \text{UInt}\langle max \rangle, \textsc{Public} \rangle \qquad \Gamma \vdash e_2 : \langle \tau, \ell_e \rangle \qquad \ell_e \leq_\ell \ell_x\end{array}}{\mathcal{M}(a, e_1) := e_2}$$

$$\frac{\begin{array}{l}\text{if } (e)\{s_1\} \text{ else } \{s_2\} \implies \\ \Gamma \vdash e : \langle bool, \ell \rangle\end{array}}{} \qquad \frac{\begin{array}{l}\text{for } (\langle \tau, \textsc{Public} \rangle i \text{ from } e_1 \text{ to } e_2)\{s\} \implies \\ i \notin \mu \qquad \Gamma \vdash e_1 : \langle \tau, \textsc{Public} \rangle \qquad \Gamma \vdash e_2 : \langle \tau, \textsc{Public} \rangle\end{array}}{}$$

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