Types

Base type		Label		Mutability	
τ	::=	ℓ	::=	σ	::=
	$\textsc{Bool}$		$\textsc{Public}$		$\textsc{Const}$
	$\textsc{UInt}\langle n\rangle$		$\textsc{Secret}$		$\textsc{Mut}$
	$\textsc{Int}\langle n\rangle$				
	$\textsc{Arr}\langle\tau, n\rangle$				

Type Lattice

$$\frac{n_1 < n_2}{\textsc{UInt}\langle n_1\rangle <_\tau \textsc{UInt}\langle n_2\rangle} \qquad \frac{n_1 < n_2}{\textsc{Int}\langle n_1\rangle <_\tau \textsc{Int}\langle n_2\rangle} \qquad \frac{}{\textsc{UInt}\langle n\rangle <_\tau \textsc{Int}\langle 2n\rangle}$$

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

$$\frac{}{\ell \cup \textsc{Secret} = \textsc{Secret}}$$

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

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

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

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

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

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

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

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

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

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

Array Initializers

$$\begin{array}{lll} \textsc{ArrInit} & & \\ \mathit{init} & ::= & \\ & \mid & \langle \tau, n \rangle \textsc{zeros} \\ & \mid & \langle \tau, n \rangle \textsc{fill}(e) \\ & \mid & \langle \tau, n \rangle x \Rightarrow e \\ & \mid & \textsc{copy}(a) \end{array}$$

$$\textsc{ZeroInit}\ \frac{\tau = \textsc{UInt}\langle s \rangle \vee \tau = \textsc{Int}\langle s \rangle}{\Gamma \vdash \langle \tau, n \rangle \textsc{zeros} : \langle \textsc{Arr}\langle \tau, n \rangle, \textsc{Public} \rangle}$$

$$\textsc{FillInit}\ \frac{\Gamma \vdash e : \langle \tau, \ell \rangle}{\Gamma \vdash \langle \tau, n \rangle \textsc{fill}(e) : \langle \textsc{Arr}\langle \tau, n \rangle, \ell \rangle}$$

$$\textsc{CompInit}\ \frac{\Gamma \vdash e : \langle \tau, \ell \rangle}{\Gamma \vdash \langle \tau, n \rangle x \Rightarrow e : \langle \textsc{Arr}\langle \tau, n \rangle, \ell \rangle}$$

$$\textsc{CopyInit}\ \frac{\mu(a) = \langle \textsc{Arr}\langle \tau, n \rangle, \ell, \sigma \rangle}{\Gamma \vdash \textsc{copy}(a) : \langle \textsc{Arr}\langle \tau, n \rangle, \ell \rangle}$$

Statements

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

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

$$\textsc{ArrDec}\ \frac{\Gamma \vdash \mathit{init} : \langle \textsc{Arr}\langle \tau, n \rangle, \ell_1 \rangle \qquad \ell_1 \leq_\ell \ell_2}{\begin{array}{c}\Sigma\langle \ell_s \rangle \vdash \langle \textsc{Arr}\langle \tau, n \rangle, \ell_2, \sigma \rangle a := \mathit{init} : \textsc{Public} \\ \mu(a) = \langle \textsc{Arr}\langle \tau, n \rangle, \ell_2, \sigma \rangle \text{ (scoping?)}\end{array}}$$

$$\textsc{ArrView}\ \frac{\mu(a) = \langle \textsc{Arr}\langle \tau, n \rangle, \ell, \sigma \rangle \qquad \Gamma \vdash e : \langle \textsc{UInt}\langle \mathit{max} \rangle, \textsc{Public} \rangle \qquad n' \leq n \qquad \ell \leq_\ell \ell' \qquad \sigma' \leq_\sigma \sigma}{\begin{array}{c}\Sigma\langle \ell_s \rangle \vdash \langle \textsc{Arr}\langle \tau, n' \rangle, \ell', \sigma' \rangle a' := \textsc{view}(a, e) : \textsc{Public} \\ \mu(a') = \langle \textsc{Arr}\langle \tau, n' \rangle, \ell', \sigma' \rangle \text{ (scoping?)}\end{array}}$$

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

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

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

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

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