Grammar

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Base type}} \\ b & ::= & \\ & \mid & \textsc{Bool} \\ & \mid & \textsc{UInt\_}n \\ & \mid & \textsc{Int\_}n \end{array} \qquad \begin{array}{lll} \multicolumn{3}{l}{\textsc{Type}} \\ \tau & ::= & \\ & \mid & b \\ & \mid & \textsc{Arr}\langle b, n\rangle \end{array} \qquad \begin{array}{lll} \multicolumn{3}{l}{\textsc{Label}} \\ \ell & ::= & \\ & \mid & \textsc{Public} \\ & \mid & \textsc{Secret} \end{array}$$

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Mutability}} \\ \sigma & ::= & \\ & \mid & \textsc{Const} \\ & \mid & \textsc{Mut} \end{array} \qquad \begin{array}{llll} \multicolumn{4}{l}{\textsc{Function argument}} \\ arg & ::= & & \\ & \mid & e & \text{by value} \\ & \mid & \textsc{Mut}\ x & \text{by reference} \end{array}$$

$$\begin{array}{llll} \multicolumn{4}{l}{\textsc{Expression}} \\ e & ::= & & \\ & \mid & \textsc{true} & \\ & \mid & \textsc{false} & \\ & \mid & c & \text{integer literal} \\ & \mid & x & \text{variable} \\ & \mid & a & \text{array} \\ & \mid & a[e] & \text{array get} \\ & \mid & \ominus e & \text{unary op} \\ & \mid & e_1 \oplus e_2 & \text{binary op} \\ & \mid & f(arg_1, \ldots, arg_n) & \text{function call} \end{array} \qquad \begin{array}{llll} \multicolumn{4}{l}{\textsc{Array}} \\ a & ::= & & \\ & \mid & \langle \tau, n\rangle x \Rightarrow e & \text{array comprehension} \\ & \mid & \textsc{view}(a, e, n) & \text{array view} \end{array}$$

$$\begin{array}{llll} \multicolumn{4}{l}{\textsc{Statement}} \\ s & ::= & & \\ & \mid & s_1; s_2 & \text{sequence} \\ & \mid & \langle \tau, \ell, \sigma\rangle x := e & \text{variable declaration} \\ & \mid & x := e & \text{variable assignment} \\ & \mid & a[e_1] = e_2 & \text{array assignment} \\ & \mid & \textsc{if}\ e\ \{s_1\}\ \textsc{else}\ \{s_2\} & \text{conditional} \\ & \mid & \textsc{for}\ \langle b\rangle x\ \textsc{from}\ e_1\ \textsc{to}\ e_2\ \{s\} & \text{loop} \\ & \mid & \textsc{return}\ e & \text{return} \end{array}$$

$$\begin{array}{lll} \multicolumn{3}{l}{\textsc{Function Definition}} \\ fdec & ::= & \\ & \mid & \langle b, \ell\rangle f(\langle \tau_1, \ell_1, \sigma_1\rangle x_1, \ldots, \langle \tau_n, \ell_n, \sigma_n\rangle x_n)\ \{s\} \end{array}$$

Type Lattice

$$\frac{n_1 < n_2}{\textsc{UInt\_}n_1 <_\tau \textsc{UInt\_}n_2} \qquad \frac{n_1 < n_2}{\textsc{Int\_}n_1 <_\tau \textsc{Int\_}n_2} \qquad \frac{}{\textsc{UInt\_}n <_\tau \textsc{Int\_}2n} \qquad \frac{}{\textsc{Public} <_\ell \textsc{Secret}}$$

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

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

$$\textsc{Var}\quad \frac{\mu(x) = \langle \tau, \ell, \sigma \rangle}{\Gamma \vdash x : \langle \tau, \ell \rangle} \qquad\qquad \textsc{Unop}\quad \frac{\Gamma \vdash e : \langle \tau_1, \ell_1 \rangle \qquad \ominus : \langle \tau_1, \ell_1 \rangle \rightarrow \langle \tau_2, \ell_2 \rangle}{\Gamma \vdash \ominus e : \langle \tau_2, \ell_2 \rangle}$$

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

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

$$\textsc{FnCall}\quad \frac{\begin{array}{c}\mathbb{F}(f) = fdec(\langle \tau_1, \ell_1, \sigma_1 \rangle x_1, \ldots, \langle \tau_n, \ell_n, \sigma_n \rangle x_n) : \langle b, \ell \rangle \\ \langle \tau_1, \ell_1, \sigma_1 \rangle x_1 \leftarrow arg_1 \qquad \cdots \qquad \langle \tau_n, \ell_n, \sigma_n \rangle x_n \leftarrow arg_n\end{array}}{\Gamma \vdash f(arg_1, \ldots, arg_n) : \langle b, \ell \rangle} \qquad\qquad \textsc{True}\quad \frac{}{\Gamma \vdash \textsc{true} : \langle \textsc{Bool}, \textsc{Public} \rangle}$$

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

$$\textsc{ArrComp}\quad \frac{\Gamma \vdash e : \langle b, \ell \rangle}{\Gamma \vdash \langle b, n \rangle x \Rightarrow e : \langle \textsc{Arr}\langle b, n \rangle, \ell \rangle}$$

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

Statements

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

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

(how to ensure no Mut view of Const array?)

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

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

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

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

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