Grammar

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

$$
\begin{array}{l}
\textsc{Mutability} \\
\sigma \quad ::= \\
\quad\mid \quad \textsc{Const} \\
\quad\mid \quad \textsc{Mut}
\end{array}
\qquad
\begin{array}{lll}
\textsc{Expression} & & \\
e \quad ::= & & \\
\quad\mid & \textsc{true} & \\
\quad\mid & \textsc{false} & \\
\quad\mid & c & \text{integer literal} \\
\quad\mid & x & \text{variable} \\
\quad\mid & x[e] & \text{array get} \\
\quad\mid & \langle \tau, n\rangle x \Rightarrow e & \text{array comprehension} \\
\quad\mid & \textsc{view}(x, e, n) & \text{array view} \\
\quad\mid & \ominus e & \text{unary op} \\
\quad\mid & e_1 \oplus e_2 & \text{binary op} \\
\quad\mid & \textsc{ref}\ x & \text{mut ref} \\
\quad\mid & f(e_1, \ldots, e_n) & \text{function call}
\end{array}
$$

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

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

Type Lattice

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

$$
\frac{}{\textsc{Mut} <_\sigma \textsc{Const}}
\qquad
\frac{\Gamma \,|\, \mu \vdash e : \langle \tau_1, \ell_1, \sigma_1\rangle \qquad \tau_1 \leq_\tau \tau_2 \qquad \ell_1 \leq_\ell \ell_2 \qquad \sigma_1 \leq_\sigma \sigma_2}{\Gamma \,|\, \mu \vdash e : \langle \tau_2, \ell_2, \sigma_2\rangle}
\qquad
\frac{}{\ell \cup \ell = \ell}
$$

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

Expressions

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

$$\frac{\Gamma \,|\, \mu \vdash e : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \ominus : \langle \tau_1, \ell_1, \sigma_1 \rangle \to \langle \tau_2, \ell_2, \sigma_2 \rangle}{\Gamma \,|\, \mu \vdash \ominus e : \langle \tau_2, \ell_2, \sigma_2 \rangle}\ \textsc{Unop}$$

$$\frac{\Gamma \,|\, \mu \vdash e_1 : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \Gamma \,|\, \mu \vdash e_2 : \langle \tau_2, \ell_2, \sigma_2 \rangle \qquad \oplus : \langle \tau_1, \ell_1, \sigma_1 \rangle \to \langle \tau_2, \ell_2, \sigma_2 \rangle \to \langle \tau_3, \ell_3, \sigma_3 \rangle}{\Gamma \,|\, \mu \vdash e_1 \oplus e_2 : \langle \tau_3, \ell_3, \sigma_3 \rangle}\ \textsc{Binop}$$

$$\frac{\mu(x) = \langle \textsc{Arr}\langle b, n \rangle, \ell, \sigma \rangle \qquad \Gamma \,|\, \mu \vdash e : \langle \textsc{UInt}, \textsc{Public}, \textsc{Const} \rangle \qquad \mathit{SMT}(e < n)}{\Gamma \,|\, \mu \vdash x[e] : \langle b, \ell, \textsc{Const} \rangle}\ \textsc{ArrGet}$$

$$\frac{\Gamma \,|\, \mu[x \mapsto \langle b, \ell, \textsc{Const} \rangle] \vdash e : \langle b, \ell, \sigma \rangle}{\Gamma \,|\, \mu \vdash \langle b, n \rangle x \Rightarrow e : \langle \textsc{Arr}\langle b, n \rangle, \ell, \textsc{Mut} \rangle}\ \textsc{ArrComp}$$

$$\frac{\mu(x) = \langle \textsc{Arr}\langle b, n \rangle, \ell, \sigma \rangle \qquad \Gamma \,|\, \mu \vdash e : \langle \textsc{UInt}, \textsc{Public}, \textsc{Const} \rangle \qquad \mathit{SMT}(e + n' < n)}{\Gamma \,|\, \mu \vdash \textsc{view}(x, e, n') : \langle \textsc{Arr}\langle b, n' \rangle, \ell, \sigma \rangle}\ \textsc{ArrView}$$

$$\frac{\mu(x) = \langle \tau, \ell, \textsc{Mut} \rangle}{\Gamma \,|\, \mu \vdash \textsc{ref}\ x : \langle \tau, \ell, \textsc{Mut} \rangle}\ \textsc{MutRef}$$

$$\frac{\begin{array}{c}\mathbb{F}(f) = \mathit{fdec}(\langle \tau_1, \ell_1, \sigma_1 \rangle, \ldots, \langle \tau_n, \ell_n, \sigma_n \rangle) : \langle \tau_f, \ell_f, \sigma_f \rangle \\ \Gamma \,|\, \mu \vdash e_1 : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \ldots \qquad \Gamma \,|\, \mu \vdash e_n : \langle \tau_n, \ell_n, \sigma_n \rangle\end{array}}{\Gamma \,|\, \mu \vdash f(e_1, \ldots, e_n) : \langle \tau_f, \ell_f, \sigma_f \rangle}\ \textsc{FnCall}$$

$$\frac{}{\Gamma \,|\, \mu \vdash \textsc{true} : \langle \textsc{Bool}, \textsc{Public}, \textsc{Const} \rangle}\ \textsc{True}$$

$$\frac{}{\Gamma \,|\, \mu \vdash \textsc{false} : \langle \textsc{Bool}, \textsc{Public}, \textsc{Const} \rangle}\ \textsc{False}$$

$$\frac{c >= 0 \qquad n = \lceil \log_2 c \rceil}{\Gamma \,|\, \mu \vdash c : \langle \textsc{UInt}_n, \textsc{Public}, \textsc{Const} \rangle}\ \textsc{PosNumber}$$

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

Statements

$$\textsc{Seq}\quad \frac{\Delta \vdash s_1 \;\rightarrow\; \Delta' \qquad \Delta' \vdash s_2 \;\rightarrow\; \Delta''}{\Delta \vdash s_1; s_2 \;\rightarrow\; \Delta''}$$

$$\textsc{VarDec}\quad \frac{x \notin Dom(\mu) \qquad \ell_s \leq_\ell \ell \qquad \Gamma \,|\, \mu \vdash e : \langle \tau, \ell, \sigma \rangle}{\langle \mu, \ell_s, r_? \rangle \vdash \langle \tau, \ell, \sigma \rangle x := e \;\rightarrow\; \langle \mu \mapsto x : \langle \tau, \ell, \sigma \rangle, \ell_s, r_? \rangle}$$

$$\textsc{VarDec*}\quad \frac{x \notin Dom(\mu) \qquad \ell_s \leq_\ell \ell \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell, \textsc{Const} \rangle}{\langle \mu, \ell_s, r_? \rangle \vdash \langle b, \ell, \textsc{Mut} \rangle x := e \;\rightarrow\; \langle \mu \mapsto x : \langle b, \ell, \textsc{Mut} \rangle, \ell_s, r_? \rangle}$$

$$\textsc{VarAssign}\quad \frac{\mu(x) = \langle b, \ell, \textsc{Mut} \rangle \qquad \Gamma \,|\, \mu \vdash e : \langle b, \ell, \textsc{Const} \rangle}{\Delta\langle \ell_s \rangle \vdash x := e : \textsc{Public}}$$

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

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

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

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