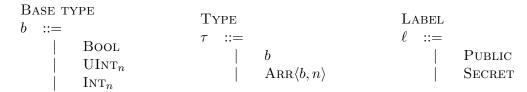
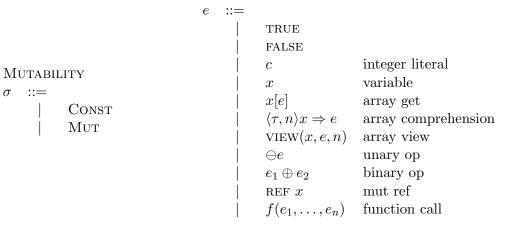
### Grammar



#### EXPRESSION



#### STATEMENT

$$\begin{array}{lll} s & \text{ ::= } & & & & & \\ & \mid & s_1; s_2 & & & \text{ sequence } \\ & \mid & \langle \tau, \ell, \sigma \rangle x := e & & \text{ variable declaration } \\ & \mid & x := e & & \text{ variable assignment } \\ & \mid & x[e_1] = e_2 & & \text{ array assignment } \\ & \mid & \text{ if } e \; \{s_1\} \; \text{ ELSE } \{s_2\} & & \text{ conditional } \\ & \mid & \text{ FOR } \langle b \rangle x \; \text{ FROM } e_1 \; \text{ TO } e_2 \; \{s\} & \text{ loop } \\ & \mid & \text{ RETURN } e & & \text{ return } \end{array}$$

# FUNCTION DEFINITION

$$fdec ::= \begin{cases} \langle b, \ell \rangle f(\langle \tau_1, \ell_1, \sigma_1 \rangle x_1, \dots, \langle \tau_n, \ell_n, \sigma_n \rangle x_n) \ \{s\} \end{cases}$$

#### Metavariables

## FUNCTION TYPE STORE

### Type Lattice

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

$$\frac{\Gamma \mid \mu \vdash e : \langle \tau_1, \ell_1, \sigma_1 \rangle \quad \tau_1 \leq_{\tau} \tau_2 \quad \ell_1 \leq_{\ell} \ell_2 \quad \sigma_1 \leq_{\sigma} \sigma_2}{\Gamma \mid \mu \vdash e : \langle \tau_2, \ell_2, \sigma_2 \rangle} \qquad \frac{\ell \cup \ell = \ell}{\ell}$$

$$\overline{\ell \cup \text{Secret} = \text{Secret}}$$
  $\overline{\text{Secret} \cup \ell = \text{Secret}}$ 

# Expressions

$$\boxed{\Gamma \, | \, \mu \, \vdash \, e : \langle \tau, \ell, \sigma \rangle}$$

$$\frac{\text{VAR}}{\mu(x) = \langle \tau, \ell, \sigma \rangle} \frac{\text{UNOP}}{\Gamma \mid \mu \vdash x : \langle \tau, \ell, \text{Const} \rangle} \qquad \frac{\Gamma \mid \mu \vdash e : \langle \tau_1, \ell_1, \sigma_1 \rangle \quad \ominus : \langle \tau_1, \ell_1, \sigma_1 \rangle \rightarrow \langle \tau_2, \ell_2, \sigma_2 \rangle}{\Gamma \mid \mu \vdash \ominus e : \langle \tau_2, \ell_2, \sigma_2 \rangle}$$

BINOP

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

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

ARRCOMP  

$$\Gamma \mid \mu[x \mapsto \langle b, \ell, \text{Const} \rangle] \vdash e : \langle b, \ell, \sigma \rangle$$

$$\frac{\Gamma \mid \mu \vdash \langle b, n \rangle_{x} \Rightarrow e : \langle ARR\langle b, n \rangle, \ell, MUT \rangle}{\Gamma \mid \mu \vdash \langle b, n \rangle_{x} \Rightarrow e : \langle ARR\langle b, n \rangle, \ell, MUT \rangle}$$

ArrView

$$\frac{\mu(x) = \langle \operatorname{Arr}\langle b, n \rangle, \ell, \sigma \rangle \qquad \Gamma \mid \mu \vdash e : \langle \operatorname{UInt}, \operatorname{Public}, \operatorname{Const} \rangle \qquad SMT(e + n' < n)}{\Gamma \mid \mu \vdash \operatorname{View}(x, e, n') : \langle \operatorname{Arr}\langle b, n' \rangle, \ell, \sigma \rangle}$$

MUTREF
$$\mu(x) = \langle \tau, \ell, \text{MUT} \rangle$$

$$\overline{\Gamma \mid \mu \vdash \text{REF } x : \langle \tau, \ell, \text{MUT} \rangle}$$

FNCALL
$$\mathbb{F}(f) = f dec(\langle \tau_1, \ell_1, \sigma_1 \rangle, \dots, \langle \tau_n, \ell_n, \sigma_n \rangle) : \langle \tau_f, \ell_f, \sigma_f \rangle$$

$$\frac{\Gamma \mid \mu \vdash e_1 : \langle \tau_1, \ell_1, \sigma_1 \rangle \qquad \Gamma \mid \mu \vdash e_n : \langle \tau_n, \ell_n, \sigma_n \rangle}{\Gamma \mid \mu \vdash f(e_1, \dots, e_n) : \langle \tau_f, \ell_f, \sigma_f \rangle}$$

True

$$\Gamma \mid \mu \vdash \text{TRUE} : \langle \text{Bool}, \text{Public}, \text{Const} \rangle$$

False 
$$\frac{c>=0 \qquad n=\lceil \log_2 c \rceil}{\Gamma \mid \mu \vdash \text{False} : \langle \text{Bool}, \text{Public}, \text{Const} \rangle}$$

$$\Gamma \mid \mu \vdash \text{false} : \langle \text{Bool}, \text{Public}, \text{Const} \rangle$$
  $\Gamma \mid \mu \vdash c : \langle \text{UInt}_n, \text{Public}, \text{Const} \rangle$ 

Negnumber 
$$\frac{c < 0}{\Gamma \mid \mu \vdash c : \langle \text{Int}_n, \text{Public}, \text{Const} \rangle}$$

**Statements** 

$$\frac{\Delta \vdash s_1 \to \Delta' \quad \Delta' \vdash s_2 \to \Delta''}{\Delta \vdash s_1; s_2 \to \Delta''}$$

VARDEC\*

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

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

ARRASSIGN

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

$$\frac{\Gamma}{\Gamma \vdash e : \langle \text{Bool}, \ell \rangle} \frac{\Delta \langle \ell \cup \ell_s \rangle \vdash s_1 : \ell_s'}{\Delta \langle \ell_s \rangle \vdash \text{if } e \ \{s_1\} \ \text{Else} \ \{s_2\} : \ell_s' \cup \ell_s''}$$

For

$$\frac{\Gamma \cup R}{\Gamma \vdash e_1 : \langle b, \text{Public} \rangle} \qquad \Gamma \vdash e_2 : \langle b, \text{Public} \rangle \qquad b = \text{UInt}_s \lor b = \text{Int}_s \qquad \Delta \langle \ell_s \rangle \vdash s : \ell_s'$$

$$\frac{\Delta \langle \ell_s \rangle \vdash \text{for } \langle b \rangle x \text{ from } e_1 \text{ to } e_2 \{s\} : \ell_s'}{\mu(x) = \langle b, \text{Public}, \text{Const} \rangle \text{ (scoping?)}}$$

$$\frac{\text{RET}}{\Gamma \vdash e : \langle b, \ell_1 \rangle} \frac{\mathbb{F}(f) = f dec : \langle b, \ell_2 \rangle}{\Delta \langle \ell_s \rangle \vdash \text{RETURN } e : \ell_s} \frac{\ell_1 \leq_{\ell} \ell_2}{\ell_2}$$