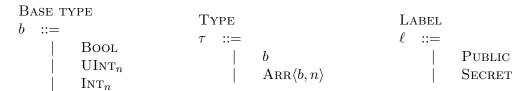
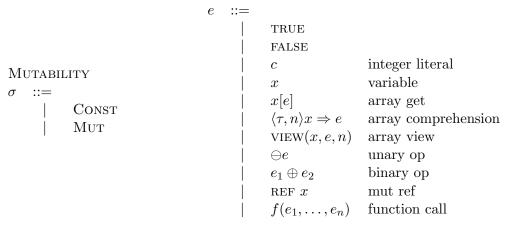
### Grammar



### EXPRESSION



# STATEMENT

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

# FUNCTION DEFINITION

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

# Type Lattice

$$\frac{n_1 < n_2}{\text{UINT}_{n_1} <_{\tau} \text{UINT}_{n_2}} \qquad \frac{n_1 < n_2}{\text{INT}_{n_1} <_{\tau} \text{INT}_{n_2}} \qquad \overline{\text{UINT}_n <_{\tau} \text{INT}_{2n}} \qquad \overline{\text{PUBLIC}} <_{\ell} \text{SECRET}$$

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

$$\overline{\ell \cup \text{SECRET} = \text{SECRET}} \qquad \overline{\text{SECRET}} \cup \ell = \overline{\text{SECRET}}$$

### Expressions

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

BINOP

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

ARRGET

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

ArrComp

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

ArrView

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

FNCALL

MUTREF
$$\frac{\mu(x) = \langle \tau, \ell, \text{MUT} \rangle}{\Gamma \mid \mu \vdash \text{REF } x : \langle \tau, \ell, \text{MUT} \rangle}$$

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

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

TRUE

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

FALSE

POSNUMBER
$$c >= 0 \qquad n = \lceil \log_2 c \rceil$$

$$\frac{\Gamma \mid u \mid c \mid c \mid \text{ULYE} \quad \text{PURITY CONST.}}{\Gamma \mid u \mid c \mid c \mid \text{ULYE}}$$

 $\Gamma \mid \mu \vdash \text{FALSE} : \langle \text{BOOL}, \text{PUBLIC}, \text{CONST} \rangle$   $\Gamma \mid \mu \vdash c : \langle \text{UInt}_n, \text{Public}, \text{Const} \rangle$ 

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
$$x \notin Dom(\mu) \qquad \ell_s \leq_{\ell} \ell \qquad \Gamma \mid \mu \vdash e : \langle \tau, \ell, \sigma \rangle$$

$$\langle \mu, \ell_s, r_7 \rangle \vdash \langle \tau, \ell, \sigma \rangle x := e \rightarrow \langle \mu \mapsto x : \langle \tau, \ell, \sigma \rangle, \ell_s, r_7 \rangle$$

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

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

# Arrassign

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

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

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

$$\Delta \langle \ell_s \rangle \vdash \text{RETURN } e : \ell_s$$