s	$::=$		Secret label
	$\mid$	$\mathcal{A}$	
	$\mid$	$\mathcal{B}$	
ℓ	$::=$		Label
	$\mid$	$\mathcal{P}$	
	$\mid$	s	
σ	$::=$		Base type
	$\mid$	uint	
	$\mid$	bool	
τ	$::=$		Type
	$\mid$	σ^{ℓ}	
	$\mid$	$\mathsf{uint}^{\ell}[\,]$	
e	$::=$		Expression
	$\mid$	n	
	$\mid$	x	
	$\mid$	$e_1 \oplus e_2$	
	$\mid$	$e_1 \mathbin{?} e_2 \;:\; e_3$	
	$\mid$	$e_1 > e_2$	
	$\mid$	$x[e]$	
	$\mid$	$e_1 \oplus_s e_2$	
	$\mid$	$\mathbf{mux}_s\ e\ e_1\ e_2$	
	$\mid$	$e_1 >_s e_2$	
	$\mid$	$e \rhd \ell$	
c	$::=$		Command
	$\mid$	$\tau\, x = e$	
	$\mid$	$x := e$	
	$\mid$	$\mathbf{for}\ x \;\in\; [n \ldots m]\ \mathbf{do}\ c$	
	$\mid$	$x[e_1] := e_2$	
	$\mid$	$\mathbf{if}\ e\ c_1\ c_2$	
	$\mid$	$\mathbf{out}\ e$	
	$\mid$	$c_1; c_2$	
Γ	$::=$		Type environment
	$\mid$	$\cdot$	
	$\mid$	$\Gamma, x : \tau$	

$$\boxed{\ell_1 \sqsubseteq \ell_2}$$

$$\frac{}{\ell \sqsubseteq \ell} \quad \text{L\_REFL}$$

$$\frac{}{\mathcal{P} \sqsubseteq s} \quad \text{L\_PS}$$

$$\frac{}{s_1 \sqsubseteq s_2} \quad \text{L\_SS}$$

$$\boxed{\Gamma \vdash e : \tau \rightsquigarrow e'}$$

$$\frac{}{\Gamma \vdash n : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow n} \quad \text{S\_CONST}$$

$$\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau \rightsquigarrow x} \quad \text{S\_VAR}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 \oplus e_2 : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_1' \oplus e_2'} \quad \text{S\_PBINOP}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{A}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 \oplus e_2 : \mathsf{uint}^{\mathcal{A}} \rightsquigarrow e_1' \oplus_{\mathcal{A}} e_2'} \quad \text{S\_SBINOP}$$

$$\frac{\begin{array}{l}\Gamma \vdash e : \mathsf{bool}^{\mathcal{P}} \rightsquigarrow e' \\ \Gamma \vdash e_i : \tau \rightsquigarrow e_i'\end{array}}{\Gamma \vdash e \mathrel{?} e_1 \ : \ e_2 : \tau \rightsquigarrow e' \mathrel{?} e_1' \ : \ e_2'} \quad \text{S\_PCOND}$$

$$\frac{\begin{array}{l}\Gamma \vdash e : \mathsf{bool}^{\mathcal{B}} \rightsquigarrow e' \\ \Gamma \vdash e_i : \tau \rightsquigarrow e_i'\end{array}}{\Gamma \vdash e \mathrel{?} e_1 \ : \ e_2 : \tau \rightsquigarrow \mathbf{mux}_{\mathcal{B}}\ e'\ e_1'\ e_2'} \quad \text{S\_SCOND}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 > e_2 : \mathsf{bool}^{\mathcal{P}} \rightsquigarrow e_1' > e_2'} \quad \text{S\_PGT}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{B}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 > e_2 : \mathsf{bool}^{\mathcal{B}} \rightsquigarrow e_1' >_{\mathcal{B}} e_2'} \quad \text{S\_SGT}$$

$$\frac{\begin{array}{l}\Gamma \vdash x : \mathsf{uint}^{\ell}[\,] \rightsquigarrow x \\ \Gamma \vdash e : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e'\end{array}}{\Gamma \vdash x[e] : \mathsf{uint}^{\ell} \rightsquigarrow x[e']} \quad \text{S\_AREAD}$$

$$\frac{\begin{array}{l}\Gamma \vdash e : \sigma^{\ell_1} \rightsquigarrow e' \\ \ell_1 \sqsubseteq \ell_2\end{array}}{\Gamma \vdash e : \sigma^{\ell_2} \rightsquigarrow e' \rhd \ell_2} \quad \text{S\_SUB}$$

$$\boxed{\Gamma \vdash c \rightsquigarrow c' \mid \Gamma'}$$

$$\frac{\Gamma \vdash e : \tau \rightsquigarrow e'}{\Gamma \vdash \tau\, x = e \rightsquigarrow \tau\, x = e' \mid \Gamma, x : \tau} \quad \text{C\_DECL}$$

$$\frac{\begin{array}{l}\Gamma(x) = \tau \\ \Gamma \vdash e : \tau \rightsquigarrow e'\end{array}}{\Gamma \vdash x := e \rightsquigarrow x := e' \mid \Gamma} \quad \text{C\_VASSGN}$$

$$\frac{\begin{array}{l}\Gamma, x : \mathsf{uint}^{\mathcal{P}} \vdash c \rightsquigarrow c' \mid \_ \\ x \notin \mathsf{modifies}(c)\end{array}}{\Gamma \vdash \mathbf{for}\ x\ \in\ [n \ldots m]\ \mathbf{do}\ c \rightsquigarrow \mathbf{for}\ x\ \in\ [n \ldots m]\ \mathbf{do}\ c' \mid \Gamma} \quad \text{C\_FOR}$$

$$\frac{\begin{array}{l}\Gamma \vdash x : \mathsf{uint}^{\ell}[\,] \rightsquigarrow x \\ \Gamma \vdash e_1 : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_1' \\ \Gamma \vdash e_2 : \mathsf{uint}^{\ell} \rightsquigarrow e_2'\end{array}}{\Gamma \vdash x[e_1] := e_2 \rightsquigarrow x[e_1'] := e_2' \mid \Gamma} \quad \text{C\_AWRITE}$$

$$\frac{\begin{array}{l}\Gamma \vdash e : \mathsf{bool}^{\mathcal{P}} \rightsquigarrow e' \\ \Gamma \vdash c_1 \rightsquigarrow c_1' \mid \_ \\ \Gamma \vdash c_2 \rightsquigarrow c_2' \mid \_\end{array}}{\Gamma \vdash \mathbf{if}\ e\ c_1\ c_2 \rightsquigarrow \mathbf{if}\ e'\ c_1'\ c_2' \mid \Gamma} \quad \text{C\_IF}$$

$$\frac{\Gamma \vdash e : \tau \rightsquigarrow e'}{\Gamma \vdash \mathbf{out}\ e \rightsquigarrow \mathbf{out}\ e' \mid \Gamma} \quad \text{C\_OUT}$$

$$\frac{\begin{array}{l}\Gamma \vdash c_1 \rightsquigarrow c_1' \mid \Gamma_1 \\ \Gamma_1 \vdash c_2 \rightsquigarrow c_2' \mid \Gamma'\end{array}}{\Gamma \vdash c_1; c_2 \rightsquigarrow c_1'; c_2' \mid \Gamma'} \quad \text{C\_SEQ}$$

$$\begin{array}{llll}
w & ::= & & \text{Runtime base values} \\
 & \mid & n & \\
 & \mid & \mathsf{true} & \\
 & \mid & \mathsf{false} & \\
 & \mid & w^{s,1} & \\
 & \mid & w^{s,2} &
\end{array}$$

$$\begin{array}{llll}
v & ::= & & \text{Runtime values} \\
 & \mid & w & \\
 & \mid & [\,\overline{v_i}^{\,i}\,] &
\end{array}$$

$$\begin{array}{llll}
\rho & ::= & & \text{Runtime environment} \\
 & \mid & \cdot & \\
 & \mid & \rho, x \mapsto v &
\end{array}$$

$$\boxed{\rho_1, \rho_2 \vdash e \Downarrow v}$$

$$\frac{}{\rho_1, \rho_2 \vdash n \Downarrow n} \quad \text{EE\_CONST}$$

$$\frac{\rho_1[x] = \rho_2[x] = v}{\rho_1, \rho_2 \vdash x \Downarrow v} \quad \text{EE\_PVAR}$$

$$\frac{\begin{array}{l} \rho_1[x] = w^{s,1} \\ \rho_2[x] = w^{s,2} \end{array}}{\rho_1, \rho_2 \vdash x \Downarrow v} \quad \text{EE\_SVAR}$$

$$\frac{\rho_1, \rho_2 \vdash e_i \Downarrow n_i}{\rho_1, \rho_2 \vdash e_1 \oplus e_2 \Downarrow n_1 \oplus n_2} \quad \text{EE\_PBINOP}$$

$$\frac{\begin{array}{l} \rho_1, \rho_2 \vdash e \Downarrow \mathsf{true} \\ \rho_1, \rho_2 \vdash e_1 \Downarrow v \end{array}}{\rho_1, \rho_2 \vdash e \,?\, e_1 \;:\; e_2 \Downarrow v} \quad \text{EE\_PCONDT}$$

$$\frac{\begin{array}{l} \rho_1, \rho_2 \vdash e \Downarrow \mathsf{false} \\ \rho_1, \rho_2 \vdash e_2 \Downarrow v \end{array}}{\rho_1, \rho_2 \vdash e \,?\, e_1 \;:\; e_2 \Downarrow v} \quad \text{EE\_PCONDF}$$

$$\frac{\rho_1, \rho_2 \vdash e_i \Downarrow n_i}{\rho_1, \rho_2 \vdash e_1 > e_2 \Downarrow n_1 > n_2} \quad \text{EE\_PGT}$$

$$\frac{\begin{array}{l} \rho_1, \rho_2 \vdash e \Downarrow n \\ \rho_1, \rho_2 \vdash x \Downarrow [\,\overline{v_i}^{\,i}\,] \end{array}}{\rho_1, \rho_2 \vdash x[e] \Downarrow v_n} \quad \text{EE\_AREAD}$$