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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

w	$::=$		Runtime base values
	$\mid$	n	
	$\mid$	true	
	$\mid$	false	
	$\mid$	$w^{s,1}$	
	$\mid$	$w^{s,2}$	

v	$::=$		Runtime values
	$\mid$	w	
	$\mid$	$[\,\overline{v_i}^{\,i}\,]$	

ρ	$::=$		Runtime environment
	$\mid$	$\cdot$	
	$\mid$	$\rho[x \mapsto v]$	

$$\boxed{\rho_1, \rho_2 \vdash e \Downarrow v_1, v_2}$$

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

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

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

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

$$\frac{\begin{array}{l}\rho_1, \rho_2 \vdash e \Downarrow \mathsf{true}, \mathsf{true} \\ \rho_1, \rho_2 \vdash e_1 \Downarrow v_1, v_2\end{array}}{\rho_1, \rho_2 \vdash e \mathrel{?} e_1 \,:\, e_2 \Downarrow v_1, v_2} \quad \text{EE\_PCONDT}$$

$$\frac{\begin{array}{l}\rho_1, \rho_2 \vdash e \Downarrow \mathsf{false}, \mathsf{false} \\ \rho_1, \rho_2 \vdash e_2 \Downarrow v_1, v_2\end{array}}{\rho_1, \rho_2 \vdash e \mathrel{?} e_1 \,:\, e_2 \Downarrow v_1, v_2} \quad \text{EE\_PCONDF}$$

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

$$\frac{\begin{array}{l}\rho_1, \rho_2 \vdash e \Downarrow n, n \\ \rho_1, \rho_2 \vdash x \Downarrow [\,\overline{v_{1\,i}}^{\,i}\,], [\,\overline{v_{2\,i}}^{\,i}\,]\end{array}}{\rho_1, \rho_2 \vdash x[e] \Downarrow v_{1\,n}, v_{2\,n}} \quad \text{EE\_AREAD}$$

$$\frac{\rho_1, \rho_2 \vdash e_i \Downarrow {n_i}^{s,1}, {n_i}^{s,2}}{\rho_1, \rho_2 \vdash e_1 \oplus_s e_2 \Downarrow (n_1 \oplus n_2)^{s,1}, (n_1 \oplus n_2)^{s,2}} \quad \text{EE\_SBINOP}$$

$$\frac{\begin{array}{l}\rho_1, \rho_2 \vdash e \Downarrow \mathsf{true}^{s,1}, \mathsf{true}^{s,2} \\ \rho_1, \rho_2 \vdash e_1 \Downarrow v_1, v_2\end{array}}{\rho_1, \rho_2 \vdash \mathbf{mux}_s\ e\ e_1\ e_2 \Downarrow v_1, v_2} \quad \text{EE\_SCONDT}$$

$$\frac{\begin{array}{l}\rho_1, \rho_2 \vdash e \Downarrow \mathsf{false}^{s,1}, \mathsf{false}^{s,2} \\ \rho_1, \rho_2 \vdash e_2 \Downarrow v_1, v_2\end{array}}{\rho_1, \rho_2 \vdash \mathbf{mux}_s\ e\ e_1\ e_2 \Downarrow v_1, v_2} \quad \text{EE\_SCONDF}$$

$$\frac{\rho_1, \rho_2 \vdash e_i \Downarrow {n_i}^{s,1}, {n_i}^{s,2}}{\rho_1, \rho_2 \vdash e_1 >_s e_2 \Downarrow (n_1 > n_2)^{s,1}, (n_1 > n_2)^{s,2}} \quad \text{EE\_SGT}$$

$$\frac{\rho_1, \rho_2 \vdash e \Downarrow v_1, v_2}{\rho_1, \rho_2 \vdash e \triangleright s \Downarrow v_1 \triangleright s, v_2 \triangleright s} \quad \text{EE\_COERCE}$$

$$\boxed{\rho_1, \rho_2 \vdash c \longrightarrow \rho_1', \rho_2'}$$

$$\frac{\rho_1, \rho_2 \vdash e \Downarrow v_1, v_2}{\rho_1, \rho_2 \vdash \tau\, x = e \longrightarrow \rho_1[x \mapsto v_1], \rho_2[x \mapsto v_2]} \quad \text{EC\_DECL}$$

$$\frac{\rho_1, \rho_2 \vdash e \Downarrow v_1, v_2}{\rho_1, \rho_2 \vdash x := e \longrightarrow \rho_1[x \mapsto v_1], \rho_2[x \mapsto v_2]} \quad \text{EC\_ASSGN}$$