

1 Formal Development

Correctness theorem that we will aim at:

If:

- $\Gamma \vdash s \rightsquigarrow \tilde{s} \mid \Gamma'$
- $\Gamma \sim \rho$
- $\rho \vdash s \longrightarrow \rho'; O$
- $\Gamma \vdash \rho \hookrightarrow \tilde{\rho}$
- $\tilde{\rho} \vdash \tilde{s} \Longrightarrow \tilde{\rho}'; \kappa$
- $\Gamma; \tilde{\rho} \vdash \rho \hookrightarrow \hat{\rho}_1, \hat{\rho}_2$

Then:

- $\hat{\rho}_1, \hat{\rho}_2 \vdash \kappa \longmapsto \hat{\rho}'_1, \hat{\rho}'_2; O$

m	$::=$	Secret label
	\mathcal{A}	
	\mathcal{B}	
ℓ	$::=$	Label
	\mathcal{P}	
	m	
σ	$::=$	Base type
	uint^ℓ	
	bool^ℓ	
τ	$::=$	Type
	σ	
	$\sigma[]$	
c	$::=$	Constant
	n	
	\top	
	\perp	
e	$::=$	Source expression
	c	
	x	
	$e_1 + e_2$	
	$\mathbf{cond}(e, e_1, e_2)$	
	$e_1 > e_2$	
	$x[e]$	
s	$::=$	Source statement
	τx	
	$x := e$	
	$\mathbf{for}(x := n_1; x \leq n_2; x := x + 1) s$	
	$x[e_1] := e_2$	
	$\mathbf{if}(e, s_1, s_2)$	
	$\mathbf{out} e$	
	$s_1; s_2$	

Figure 1: Source language

v	$::=$	Source value
	$\begin{array}{ c} c \\ \hline [\overline{c_i}^i] \end{array}$	
ρ	$::=$	Source runtime environment
	$\begin{array}{ c} \cdot \\ \hline \rho[x \mapsto v] \end{array}$	
O	$::=$	Source observation
	$\begin{array}{ c} \cdot \\ \hline v \\ \hline O_1, O_2 \end{array}$	

Figure 2: Source runtime

$$\boxed{\rho \vdash e \downarrow v}$$

$$\begin{array}{c}
\frac{}{\rho \vdash c \downarrow c} \quad \text{SE_CONST} \\
\\
\frac{}{\rho \vdash x \downarrow \rho[x]} \quad \text{SE_VAR} \\
\\
\frac{\rho \vdash e_i \downarrow n_i}{\rho \vdash e_1 + e_2 \downarrow n_1 + n_2} \quad \text{SE_ADD} \\
\\
\frac{\rho \vdash e \downarrow \top \quad \rho \vdash e_1 \downarrow v}{\rho \vdash \mathbf{cond}(e, e_1, e_2) \downarrow v} \quad \text{SE_CONDT} \\
\\
\frac{\rho \vdash e \downarrow \perp \quad \rho \vdash e_2 \downarrow v}{\rho \vdash \mathbf{cond}(e, e_1, e_2) \downarrow v} \quad \text{SE_CONDF} \\
\\
\frac{\rho \vdash e_i \downarrow n_i}{\rho \vdash e_1 > e_2 \downarrow n_1 > n_2} \quad \text{SE_GT} \\
\\
\frac{\rho \vdash e \downarrow n \quad \rho \vdash x \downarrow [\overline{c_i}^i]}{\rho \vdash x[e] \downarrow c_n} \quad \text{SE_AREAD}
\end{array}$$

Figure 3: Source expression evaluation

$$\boxed{\rho \vdash s \longrightarrow \rho'; O}$$

$$\begin{array}{c}
\frac{\text{default}(\tau) = v}{\rho \vdash \tau x \longrightarrow \rho[x \mapsto v]; \cdot} \quad \text{SC_DECL} \\
\\
\frac{\rho \vdash e \downarrow v}{\rho \vdash x := e \longrightarrow \rho[x \mapsto v]; \cdot} \quad \text{SC_ASSGN} \\
\\
\frac{n_1 > n_2}{\rho \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) s \longrightarrow \rho; \cdot} \quad \text{SC_FORT} \\
\\
\frac{\begin{array}{l} n_2 \geq n_1 \\ \rho[x \mapsto n_1] \vdash s \longrightarrow \rho_1; O_1 \\ \rho_1 \vdash \mathbf{for}(x := n_1 + 1; x \leq n_2; x := x + 1) s \longrightarrow \rho_2; O_2 \end{array}}{\rho \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) s \longrightarrow \rho_2; O_1, O_2} \quad \text{SC_FORI} \\
\\
\frac{\begin{array}{l} \rho \vdash x \downarrow [\overline{c_i}^i] \\ \rho \vdash e_1 \downarrow n \\ \rho \vdash e_2 \downarrow c \end{array}}{\rho \vdash x[e_1] := e_2 \longrightarrow \rho[x \mapsto [\overline{c_i}^i][n \mapsto c]]; O_1, O_2} \quad \text{SC_AWRITE} \\
\\
\frac{\begin{array}{l} \rho \vdash e \downarrow \top \\ \rho \vdash s_1 \longrightarrow \rho'; O \end{array}}{\rho \vdash \mathbf{if}(e, s_1, s_2) \longrightarrow \rho'; O} \quad \text{SC_IFT} \\
\\
\frac{\begin{array}{l} \rho \vdash e \downarrow \perp \\ \rho \vdash s_2 \longrightarrow \rho'; O \end{array}}{\rho \vdash \mathbf{if}(e, s_1, s_2) \longrightarrow \rho'; O} \quad \text{SC_IFF} \\
\\
\frac{\rho \vdash e \downarrow v}{\rho \vdash \mathbf{out} e \longrightarrow \rho; v} \quad \text{SC_OUT} \\
\\
\frac{\begin{array}{l} \rho \vdash s_1 \longrightarrow \rho_1; O_1 \\ \rho_1 \vdash s_2 \longrightarrow \rho_2; O_2 \end{array}}{\rho \vdash s_1; s_2 \longrightarrow \rho_2; O_1, O_2} \quad \text{SC_SEQ}
\end{array}$$

Figure 4: Source command evaluation

$$\boxed{v : \tau}$$

$$\frac{}{n : \text{uint}^{\mathcal{P}}} \quad \text{V_INT}$$

$$\frac{}{\top : \text{bool}^{\mathcal{P}}} \quad \text{V_TRUE}$$

$$\frac{}{\perp : \text{bool}^{\mathcal{P}}} \quad \text{V_FALSE}$$

$$\frac{c_i : \sigma}{[\overline{c_i}^i] : \sigma[]} \quad \text{V_ARR}$$

Figure 5: Value typing

\tilde{e}	$::=$	$\begin{array}{ l} c \\ x \\ \tilde{e}_1 +_{\ell} \tilde{e}_2 \\ \mathbf{cond}_{\ell}(\tilde{e}, \tilde{e}_1, \tilde{e}_2) \\ \tilde{e}_1 >_{\ell} \tilde{e}_2 \\ x[\tilde{e}] \\ \tilde{e} \triangleright m \end{array}$	Target expression
\tilde{s}	$::=$	$\begin{array}{ l} \tau x \\ x := \tilde{e} \\ \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) \tilde{s} \\ x[\tilde{e}_1] := \tilde{e}_2 \\ \mathbf{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2) \\ \mathbf{out} \tilde{e} \\ \tilde{s}_1; \tilde{s}_2 \end{array}$	Target statement
Γ	$::=$	$\begin{array}{ l} . \\ \Gamma, x : \tau \end{array}$	Type environment

Figure 6: Target language

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

$$\begin{array}{c}
\frac{}{\Gamma \vdash n : \text{uint}^{\mathcal{P}} \rightsquigarrow n} \quad \text{S_CONST} \\
\\
\frac{}{\Gamma \vdash \top : \text{bool}^{\mathcal{P}} \rightsquigarrow \top} \quad \text{S_TRUE} \\
\\
\frac{}{\Gamma \vdash \perp : \text{bool}^{\mathcal{P}} \rightsquigarrow \perp} \quad \text{S_FALSE} \\
\\
\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau \rightsquigarrow x} \quad \text{S_VAR} \\
\\
\frac{\Gamma \vdash e_i : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash e_1 + e_2 : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}_1 +_{\mathcal{P}} \tilde{e}_2} \quad \text{S_PADD} \\
\\
\frac{\Gamma \vdash e_i : \text{uint}^{\mathcal{A}} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash e_1 + e_2 : \text{uint}^{\mathcal{A}} \rightsquigarrow \tilde{e}_1 +_{\mathcal{A}} \tilde{e}_2} \quad \text{S_SADD} \\
\\
\frac{\Gamma \vdash e : \text{bool}^{\mathcal{P}} \rightsquigarrow \tilde{e} \quad \Gamma \vdash e_i : \sigma \rightsquigarrow \tilde{e}_i}{\Gamma \vdash \mathbf{cond}(e, e_1, e_2) : \sigma \rightsquigarrow \mathbf{cond}_{\mathcal{P}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2)} \quad \text{S_PCOND} \\
\\
\frac{\Gamma \vdash e : \text{bool}^{\mathcal{B}} \rightsquigarrow \tilde{e} \quad \Gamma \vdash e_i : \sigma \rightsquigarrow \tilde{e}_i \quad \text{label}(\sigma) = \mathcal{B}}{\Gamma \vdash \mathbf{cond}(e, e_1, e_2) : \sigma \rightsquigarrow \mathbf{cond}_{\mathcal{B}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2)} \quad \text{S_SCOND} \\
\\
\frac{\Gamma \vdash e_i : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash e_1 > e_2 : \text{bool}^{\mathcal{P}} \rightsquigarrow \tilde{e}_1 >_{\mathcal{P}} \tilde{e}_2} \quad \text{S_PGT} \\
\\
\frac{\Gamma \vdash e_i : \text{uint}^{\mathcal{B}} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash e_1 > e_2 : \text{bool}^{\mathcal{B}} \rightsquigarrow \tilde{e}_1 >_{\mathcal{B}} \tilde{e}_2} \quad \text{S_SGT} \\
\\
\frac{\Gamma \vdash x : \sigma[\] \rightsquigarrow x \quad \Gamma \vdash e : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}}{\Gamma \vdash x[e] : \sigma \rightsquigarrow x[\tilde{e}]} \quad \text{S_AREAD} \\
\\
\frac{\Gamma \vdash e : \sigma_1 \rightsquigarrow \tilde{e} \quad \text{base}(\sigma_1) = \text{base}(\sigma_2) \quad \text{label}(\sigma_2) = m}{\Gamma \vdash e : \sigma_2 \rightsquigarrow \tilde{e} \triangleright m} \quad \text{S_SUB}
\end{array}$$

Figure 7: Expression compilation

$$\boxed{\Gamma \vdash s \rightsquigarrow \tilde{s} \mid \Gamma'}$$

$$\begin{array}{c}
\overline{\Gamma \vdash \tau x \rightsquigarrow \tau x \mid \Gamma, x : \tau} \quad \text{C_DECL} \\
\\
\frac{\Gamma(x) = \sigma \quad \Gamma \vdash e : \sigma \rightsquigarrow \tilde{e}}{\Gamma \vdash x := e \rightsquigarrow x := \tilde{e} \mid \Gamma} \quad \text{C_VASSGN} \\
\\
\frac{\Gamma, x : \text{uint}^{\mathcal{P}} \vdash s \rightsquigarrow \tilde{s} \mid _ \quad x \notin \text{modifies}(s)}{\Gamma \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) s \rightsquigarrow \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) \tilde{s} \mid \Gamma} \quad \text{C_FOR} \\
\\
\frac{\Gamma \vdash x : \sigma[_] \rightsquigarrow x \quad \Gamma \vdash e_1 : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}_1 \quad \Gamma \vdash e_2 : \sigma \rightsquigarrow \tilde{e}_2}{\Gamma \vdash x[e_1] := e_2 \rightsquigarrow x[\tilde{e}_1] := \tilde{e}_2 \mid \Gamma} \quad \text{C_AWRITE} \\
\\
\frac{\Gamma \vdash e : \text{bool}^{\mathcal{P}} \rightsquigarrow \tilde{e} \quad \Gamma \vdash s_i \rightsquigarrow \tilde{s}_i \mid _}{\Gamma \vdash \mathbf{if}(e, s_1, s_2) \rightsquigarrow \mathbf{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2) \mid \Gamma} \quad \text{C_IF} \\
\\
\frac{\Gamma \vdash e : \sigma \rightsquigarrow \tilde{e} \quad \text{label}(\sigma) = m}{\Gamma \vdash \mathbf{out} e \rightsquigarrow \mathbf{out} \tilde{e} \mid \Gamma} \quad \text{C_OUT} \\
\\
\frac{\Gamma \vdash s_1 \rightsquigarrow \tilde{s}_1 \mid \Gamma_1 \quad \Gamma_1 \vdash s_2 \rightsquigarrow \tilde{s}_2 \mid \Gamma'}{\Gamma \vdash s_1; s_2 \rightsquigarrow \tilde{s}_1; \tilde{s}_2 \mid \Gamma'} \quad \text{C_SEQ}
\end{array}$$

Figure 8: Command compilation

r	$::=$	Wire id range
\tilde{w}	$::=$	Compiled base value
	$\begin{array}{ l} c \\ r \end{array}$	
\tilde{v}	$::=$	Compiled value
	$\begin{array}{ l} \tilde{w} \\ [\widetilde{w_i}^i] \end{array}$	
κ	$::=$	Circuit
	$\begin{array}{ l} \cdot \\ \oplus(r_1, r_2, r_3) \\ \mathbf{Mux}(r_1, r_2, r_3, r_4) \\ \mathbf{Gt}(r_1, r_2, r_3) \\ r_1 \triangleright_m r_2 \\ \mathbf{Out}(r) \\ \kappa_1, \kappa_2 \end{array}$	
$\tilde{\rho}$	$::=$	Runtime environment
	$\begin{array}{ l} \cdot \\ \tilde{\rho}[x \mapsto \tilde{v}] \end{array}$	

Figure 9: Target runtime

$$\boxed{\tilde{\rho} \vdash \tilde{e} \Downarrow \tilde{v}; \kappa}$$

$$\begin{array}{c}
\frac{}{\tilde{\rho} \vdash c \Downarrow c; \cdot} \text{EE_CONST} \\
\\
\frac{}{\tilde{\rho} \vdash x \Downarrow \tilde{\rho}[x]; \cdot} \text{EE_VAR} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e}_i \Downarrow n_i; \kappa_i}{\tilde{\rho} \vdash \tilde{e}_1 +_{\mathcal{P}} \tilde{e}_2 \Downarrow n_1 + n_2; \kappa_1, \kappa_2} \text{EE_PADD} \\
\\
\frac{\begin{array}{c} \tilde{\rho} \vdash \tilde{e}_i \Downarrow r_i; \kappa_i \\ r_3 = \text{next_range}() \end{array}}{\tilde{\rho} \vdash \tilde{e}_1 +_{\mathcal{A}} \tilde{e}_2 \Downarrow r_3; \kappa_1, \kappa_2, \oplus(r_1, r_2, r_3)} \text{EE_SADD} \\
\\
\frac{\begin{array}{c} \tilde{\rho} \vdash \tilde{e} \Downarrow \top; \kappa \\ \tilde{\rho} \vdash \tilde{e}_1 \Downarrow \tilde{v}; \kappa_1 \end{array}}{\tilde{\rho} \vdash \mathbf{cond}_{\mathcal{P}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2) \Downarrow \tilde{v}; \kappa, \kappa_1} \text{EE_PCONDT} \\
\\
\frac{\begin{array}{c} \tilde{\rho} \vdash \tilde{e} \Downarrow \perp; \kappa \\ \tilde{\rho} \vdash \tilde{e}_2 \Downarrow \tilde{v}; \kappa_2 \end{array}}{\tilde{\rho} \vdash \mathbf{cond}_{\mathcal{P}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2) \Downarrow \tilde{v}; \kappa, \kappa_2} \text{EE_PCONDF} \\
\\
\frac{\begin{array}{c} \tilde{\rho} \vdash \tilde{e} \Downarrow r; \kappa \\ \tilde{\rho} \vdash \tilde{e}_i \Downarrow r_i; \kappa_i \\ r_3 = \text{next_range}() \end{array}}{\tilde{\rho} \vdash \mathbf{cond}_{\mathcal{B}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2) \Downarrow r_3; \kappa, \kappa_1, \kappa_2, \text{Mux}(r, r_1, r_2, r_3)} \text{EE_SCOND} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e}_i \Downarrow n_i; \kappa_i}{\tilde{\rho} \vdash \tilde{e}_1 >_{\mathcal{P}} \tilde{e}_2 \Downarrow n_1 > n_2; \kappa_1, \kappa_2} \text{EE_PGT} \\
\\
\frac{\begin{array}{c} \tilde{\rho} \vdash \tilde{e}_i \Downarrow r_i; \kappa_i \\ r_3 = \text{next_range}() \end{array}}{\tilde{\rho} \vdash \tilde{e}_1 >_{\mathcal{B}} \tilde{e}_2 \Downarrow r_3; \kappa_1, \kappa_2, \text{Gt}(r_1, r_2, r_3)} \text{EE_SGT} \\
\\
\frac{\begin{array}{c} \tilde{\rho} \vdash \tilde{e} \Downarrow n; \kappa_1 \\ \tilde{\rho} \vdash x \Downarrow [\widetilde{w}_i^i]; \kappa_2 \end{array}}{\tilde{\rho} \vdash x[\tilde{e}] \Downarrow \widetilde{w}_n; \kappa_1, \kappa_2} \text{EE_AREAD} \\
\\
\frac{\begin{array}{c} \tilde{\rho} \vdash \tilde{e} \Downarrow r; \kappa \\ r' = \text{next_range}() \end{array}}{\tilde{\rho} \vdash \tilde{e} \triangleright m \Downarrow r'; \kappa, r \triangleright_m r'} \text{EE_COERCE}
\end{array}$$

Figure 10: Target expression evaluation

$$\boxed{\tilde{\rho} \vdash \tilde{s} \Longrightarrow \tilde{\rho}'; \kappa}$$

$$\begin{array}{c}
\frac{\text{default}(\tau) = \tilde{v}; \kappa}{\tilde{\rho} \vdash \tau x \Longrightarrow \tilde{\rho}[x \mapsto \tilde{v}]; \kappa} \text{ EC_DECL} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow \tilde{v}; \kappa}{\tilde{\rho} \vdash x := \tilde{e} \Longrightarrow \tilde{\rho}[x \mapsto \tilde{v}]; \kappa} \text{ EC_ASSGN} \\
\\
\frac{n_1 > n_2}{\tilde{\rho} \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) \tilde{s} \Longrightarrow \tilde{\rho}; \cdot} \text{ EC_FORT} \\
\\
\frac{\begin{array}{l} n_2 \geq n_1 \\ \tilde{\rho}[x \mapsto n_1] \vdash \tilde{s} \Longrightarrow \tilde{\rho}_1; \kappa_1 \\ \tilde{\rho}_1 \vdash \mathbf{for}(x := n_1 + 1; x \leq n_2; x := x + 1) \tilde{s} \Longrightarrow \tilde{\rho}_2; \kappa_2 \end{array}}{\tilde{\rho} \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) \tilde{s} \Longrightarrow \tilde{\rho}_2; \kappa_1, \kappa_2} \text{ EC_FORI} \\
\\
\frac{\begin{array}{l} \tilde{\rho} \vdash x \Downarrow [\tilde{w}_i^i]; \cdot \\ \tilde{\rho} \vdash \tilde{e}_1 \Downarrow n; \kappa_1 \\ \tilde{\rho} \vdash \tilde{e}_2 \Downarrow \tilde{w}; \kappa_2 \end{array}}{\tilde{\rho} \vdash x[\tilde{e}_1] := \tilde{e}_2 \Longrightarrow \tilde{\rho}[x \mapsto [\tilde{w}_i^i][n \mapsto \tilde{w}]]; \kappa_1, \kappa_2} \text{ EC_AWRITE} \\
\\
\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{e} \Downarrow \top; \kappa_1 \\ \tilde{\rho} \vdash \tilde{s}_1 \Longrightarrow \tilde{\rho}'; \kappa_2 \end{array}}{\tilde{\rho} \vdash \mathbf{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2) \Longrightarrow \tilde{\rho}'; \kappa_1, \kappa_2} \text{ EC_IFT} \\
\\
\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{e} \Downarrow \perp; \kappa_1 \\ \tilde{\rho} \vdash \tilde{s}_2 \Longrightarrow \tilde{\rho}'; \kappa_2 \end{array}}{\tilde{\rho} \vdash \mathbf{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2) \Longrightarrow \tilde{\rho}'; \kappa_1, \kappa_2} \text{ EC_IFF} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow r; \kappa}{\tilde{\rho} \vdash \mathbf{out} \tilde{e} \Longrightarrow \tilde{\rho}; \kappa, \text{Out}(r)} \text{ EC_OUT} \\
\\
\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{s}_1 \Longrightarrow \tilde{\rho}_1; \kappa_1 \\ \tilde{\rho}_1 \vdash \tilde{s}_2 \Longrightarrow \tilde{\rho}_2; \kappa_2 \end{array}}{\tilde{\rho} \vdash \tilde{s}_1; \tilde{s}_2 \Longrightarrow \tilde{\rho}_2; \kappa_1, \kappa_2} \text{ EC_SEQ}
\end{array}$$

Figure 11: Target command evaluation

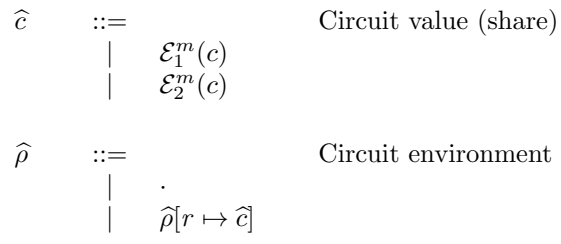


Figure 12: Circuit runtime

$$\boxed{\hat{\rho}_1, \hat{\rho}_2 \vdash \kappa \mapsto \hat{\rho}'_1, \hat{\rho}'_2; O}$$

$$\frac{}{\hat{\rho}_1, \hat{\rho}_2 \vdash \cdot \mapsto \hat{\rho}_1, \hat{\rho}_2; \cdot} \text{CKT_EMP}$$

$$\frac{\begin{array}{l} \hat{\rho}_1[r_1] = \mathcal{E}_1^A(n_1) \\ \hat{\rho}_2[r_1] = \mathcal{E}_2^A(n_1) \\ \hat{\rho}_1[r_2] = \mathcal{E}_1^A(n_2) \\ \hat{\rho}_2[r_2] = \mathcal{E}_2^A(n_2) \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \oplus(r_1, r_2, r_3) \mapsto \hat{\rho}_1[r_3 \mapsto \mathcal{E}_1^A((n_1 + n_2))], \hat{\rho}_2[r_3 \mapsto \mathcal{E}_2^A((n_1 + n_2))]; \cdot} \text{CKT_ADD}$$

$$\frac{\begin{array}{l} \hat{\rho}_1[r_1] = \mathcal{E}_1^B(\top) \\ \hat{\rho}_2[r_1] = \mathcal{E}_2^B(\top) \\ \hat{\rho}_1[r_2] = \mathcal{E}_1^B(c) \\ \hat{\rho}_2[r_2] = \mathcal{E}_2^B(c) \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \text{Mux}(r_1, r_2, r_3, r_4) \mapsto \hat{\rho}_1[r_4 \mapsto \mathcal{E}_1^B(c)], \hat{\rho}_2[r_4 \mapsto \mathcal{E}_2^B(c)]; \cdot} \text{CKT_MUXT}$$

$$\frac{\begin{array}{l} \hat{\rho}_1[r_1] = \mathcal{E}_1^B(\perp) \\ \hat{\rho}_2[r_1] = \mathcal{E}_2^B(\perp) \\ \hat{\rho}_1[r_3] = \mathcal{E}_1^B(c) \\ \hat{\rho}_2[r_3] = \mathcal{E}_2^B(c) \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \text{Mux}(r_1, r_2, r_3, r_4) \mapsto \hat{\rho}_1[r_4 \mapsto \mathcal{E}_1^B(c)], \hat{\rho}_2[r_4 \mapsto \mathcal{E}_2^B(c)]; \cdot} \text{CKT_MUXF}$$

$$\frac{\begin{array}{l} \hat{\rho}_1[r_1] = \mathcal{E}_1^B(n_1) \\ \hat{\rho}_2[r_1] = \mathcal{E}_2^B(n_1) \\ \hat{\rho}_1[r_2] = \mathcal{E}_1^B(n_2) \\ \hat{\rho}_2[r_2] = \mathcal{E}_2^B(n_2) \\ c = n_1 > n_2 \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \text{Gt}(r_1, r_2, r_3) \mapsto \hat{\rho}_1[r_3 \mapsto \mathcal{E}_1^B(c)], \hat{\rho}_2[r_3 \mapsto \mathcal{E}_2^B(c)]; \cdot} \text{CKT_GT}$$

$$\frac{\begin{array}{l} \hat{\rho}_1[r_1] = \mathcal{E}_1^{m_1}(c) \\ \hat{\rho}_2[r_1] = \mathcal{E}_2^{m_1}(c) \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash r_1 \triangleright_m r_2 \mapsto \hat{\rho}_1[r_2 \mapsto \mathcal{E}_1^m(c)], \hat{\rho}_2[r_2 \mapsto \mathcal{E}_2^m(c)]; \cdot} \text{CKT_COERCE}$$

$$\frac{\begin{array}{l} \hat{\rho}_1[r] = \mathcal{E}_1^m(c) \\ \hat{\rho}_2[r] = \mathcal{E}_2^m(c) \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \text{Out}(r) \mapsto \hat{\rho}_1, \hat{\rho}_2; c} \text{CKT_OUT}$$

$$\frac{\begin{array}{l} \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa_1 \mapsto \hat{\rho}'_1, \hat{\rho}'_2; O_1 \\ \hat{\rho}'_1, \hat{\rho}'_2 \vdash \kappa_2 \mapsto \hat{\rho}''_1, \hat{\rho}''_2; O_2 \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \kappa_1, \kappa_2 \mapsto \hat{\rho}''_1, \hat{\rho}''_2; O_1, O_2} \text{CKT_SEQ}$$

Figure 13: Circuit evaluation

$$\boxed{\Gamma \sim \rho}$$

$$\frac{}{\cdot \sim \cdot} \quad \text{SEN_EMP}$$

$$\frac{v : [\tau]_{\mathcal{P}} \quad \Gamma \sim \rho}{\Gamma, x : \tau \sim \rho[x \mapsto v]} \quad \text{SEN_BND}$$

Figure 14: Source environment and type environment consistency

$$\boxed{\Gamma \vdash \rho \hookrightarrow \tilde{\rho}}$$

$$\frac{}{\Gamma \vdash \cdot \hookrightarrow \cdot} \quad \text{TEN_EMP}$$

$$\frac{\Gamma(x) = \sigma \quad \text{label}(\sigma) = \mathcal{P} \quad \Gamma \vdash \rho \hookrightarrow \tilde{\rho}}{\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \tilde{\rho}[x \mapsto c]} \quad \text{TEN_PBT}$$

$$\frac{\Gamma(x) = \sigma \quad \text{label}(\sigma) = m \quad r = \text{next_range}() \quad \Gamma \vdash \rho \hookrightarrow \tilde{\rho}}{\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \tilde{\rho}[x \mapsto r]} \quad \text{TEN_SBT}$$

$$\frac{\Gamma(x) = \sigma[] \quad \text{label}(\sigma) = \mathcal{P} \quad \Gamma \vdash \rho \hookrightarrow \tilde{\rho}}{\Gamma \vdash \rho[x \mapsto [\overline{c_i}^i]] \hookrightarrow \tilde{\rho}[x \mapsto [\overline{c_i}^i]]} \quad \text{TEN_PARR}$$

$$\frac{\Gamma(x) = \sigma[] \quad \text{label}(\sigma) = m \quad r_i = \text{next_range}() \quad \Gamma \vdash \rho \hookrightarrow \tilde{\rho}}{\Gamma \vdash \rho[x \mapsto [\overline{c_i}^i]] \hookrightarrow \tilde{\rho}[x \mapsto [\overline{r_i}^i]]} \quad \text{TEN_SARR}$$

Figure 15: Source environment to target environment compilation

$$\boxed{\Gamma; \tilde{\rho} \vdash \rho \hookrightarrow \hat{\rho}_1, \hat{\rho}_2}$$

$$\begin{array}{c}
\overline{\Gamma; \tilde{\rho} \vdash \cdot \hookrightarrow \cdot, \cdot} \quad \text{CEN_EMP} \\
\\
\frac{\begin{array}{c} \Gamma(x) = \sigma \\ \text{label}(\sigma) = \mathcal{P} \\ \Gamma; \tilde{\rho} \vdash \rho \hookrightarrow \hat{\rho}_1, \hat{\rho}_2 \end{array}}{\Gamma; \tilde{\rho} \vdash \rho[x \mapsto c] \hookrightarrow \hat{\rho}_1, \hat{\rho}_2} \quad \text{CEN_PBT} \\
\\
\frac{\begin{array}{c} \Gamma(x) = \sigma \\ \text{label}(\sigma) = m \\ \tilde{\rho}[x] = r \\ \Gamma; \tilde{\rho} \vdash \rho \hookrightarrow \hat{\rho}_1, \hat{\rho}_2 \end{array}}{\Gamma; \tilde{\rho} \vdash \rho[x \mapsto c] \hookrightarrow \hat{\rho}_1[r \mapsto \mathcal{E}_1^m(c)], \hat{\rho}_2[r \mapsto \mathcal{E}_2^m(c)]} \quad \text{CEN_SBT} \\
\\
\frac{\begin{array}{c} \Gamma(x) = \sigma[] \\ \text{label}(\sigma) = \mathcal{P} \\ \Gamma; \tilde{\rho} \vdash \rho \hookrightarrow \hat{\rho}_1, \hat{\rho}_2 \end{array}}{\Gamma; \tilde{\rho} \vdash \rho[x \mapsto [\bar{c}_i^i]] \hookrightarrow \hat{\rho}_1, \hat{\rho}_2} \quad \text{CEN_PARR} \\
\\
\frac{\begin{array}{c} \Gamma(x) = \sigma[] \\ \text{label}(\sigma) = m \\ \tilde{\rho}[x] = [\bar{r}_i^i] \\ \Gamma; \tilde{\rho} \vdash \rho \hookrightarrow \hat{\rho}_1, \hat{\rho}_2 \end{array}}{\Gamma; \tilde{\rho} \vdash \rho[x \mapsto [\bar{c}_i^i]] \hookrightarrow \hat{\rho}_1[r_i \mapsto \mathcal{E}_1^m(c_i)], \hat{\rho}_2[r_i \mapsto \mathcal{E}_2^m(c_i)]} \quad \text{CEN_SARR}
\end{array}$$

Figure 16: Source environment to circuit environment compilation