1 Formal Development

Correctness theorem that we will aim at:

If:

- $\Gamma \vdash s \rightsquigarrow \widetilde{s} \mid \Gamma'$

- $\Gamma \sim \rho$

- $\rho \vdash s \longrightarrow \rho'; O$

- $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}$

- $\widetilde{\rho} \vdash \widetilde{s} \Longrightarrow \widetilde{\rho}'; \kappa$

- $\Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2$

Then:

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

$$
\begin{array}{llll}
m & ::= & & \text{Secret label} \\
& | & \mathcal{A} & \\
& | & \mathcal{B} & \\
\\
\ell & ::= & & \text{Label} \\
& | & \mathcal{P} & \\
& | & m & \\
\\
\sigma & ::= & & \text{Base type} \\
& | & \mathsf{uint}^{\ell} & \\
& | & \mathsf{bool}^{\ell} & \\
\\
\tau & ::= & & \text{Type} \\
& | & \sigma & \\
& | & \sigma[\,] & \\
\\
c & ::= & & \text{Constant} \\
& | & n & \\
& | & \top & \\
& | & \bot & \\
\\
e & ::= & & \text{Source expression} \\
& | & c & \\
& | & x & \\
& | & e_1 + e_2 & \\
& | & \mathbf{cond}(e, e_1, e_2) & \\
& | & e_1 > e_2 & \\
& | & x[e] & \\
\\
s & ::= & & \text{Source statement} \\
& | & \tau\, x & \\
& | & x := e & \\
& | & \mathbf{for}(x := n_1; x \leq n_2; x := x + 1)\, s & \\
& | & x[e_1] := e_2 & \\
& | & \mathbf{if}(e, s_1, s_2) & \\
& | & \mathbf{out}\, e & \\
& | & s_1; s_2 & \\
\end{array}
$$

Figure 1: Source language

$$v \quad ::= \quad \text{Source value}$$
$$| \quad c$$
$$| \quad [\,\overline{c_i}^{\,i}\,]$$

$$\rho \quad ::= \quad \text{Source runtime environment}$$
$$| \quad .$$
$$| \quad \rho[x \mapsto v]$$

$$O \quad ::= \quad \text{Source observation}$$
$$| \quad .$$
$$| \quad v$$
$$| \quad O_1, O_2$$

Figure 2: Source runtime

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

$$\frac{}{\rho \vdash c \downarrow c} \quad \text{SE\_CONST}$$

$$\frac{}{\rho \vdash x \downarrow \rho[x]} \quad \text{SE\_VAR}$$

$$\frac{\rho \vdash e_i \downarrow n_i}{\rho \vdash e_1 + e_2 \downarrow n_1 + n_2} \quad \text{SE\_ADD}$$

$$\frac{\rho \vdash e \downarrow \top \quad \rho \vdash e_1 \downarrow v}{\rho \vdash \mathbf{cond}(e, e_1, e_2) \downarrow v} \quad \text{SE\_CONDT}$$

$$\frac{\rho \vdash e \downarrow \bot \quad \rho \vdash e_2 \downarrow v}{\rho \vdash \mathbf{cond}(e, e_1, e_2) \downarrow v} \quad \text{SE\_CONDF}$$

$$\frac{\rho \vdash e_i \downarrow n_i}{\rho \vdash e_1 > e_2 \downarrow n_1 > n_2} \quad \text{SE\_GT}$$

$$\frac{\rho \vdash e \downarrow n \quad \rho \vdash x \downarrow [\,\overline{c_i}^{\,i}\,]}{\rho \vdash x[e] \downarrow c_n} \quad \text{SE\_AREAD}$$

Figure 3: Source expression evaluation

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

$$\frac{\mathsf{default}(\tau) = v}{\rho \vdash \tau\, x \longrightarrow \rho[x \mapsto v]; \cdot} \quad \text{SC\_DECL}$$

$$\frac{\rho \vdash e \downarrow v}{\rho \vdash x := e \longrightarrow \rho[x \mapsto v]; \cdot} \quad \text{SC\_ASSGN}$$

$$\frac{n_1 > n_2}{\rho \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1)\ s \longrightarrow \rho; \cdot} \quad \text{SC\_FORT}$$

$$\frac{\begin{array}{l} n_2 \geq n_1 \\ \rho[x \mapsto n_1] \vdash s \longrightarrow \rho_1; O_1 \\ \rho_1 \vdash \mathbf{for}(x := n_1 + 1; x \leq n_2; x := x + 1)\ s \longrightarrow \rho_2; O_2 \end{array}}{\rho \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1)\ s \longrightarrow \rho_2; O_1, O_2} \quad \text{SC\_FORI}$$

$$\frac{\begin{array}{c} \rho \vdash x \downarrow [\,\overline{c_i}^{\,i}\,] \\ \rho \vdash e_1 \downarrow n \\ \rho \vdash e_2 \downarrow c \end{array}}{\rho \vdash x[e_1] := e_2 \longrightarrow \rho[x \mapsto [\,\overline{c_i}^{\,i}\,][n \mapsto c]]; O_1, O_2} \quad \text{SC\_AWRITE}$$

$$\frac{\begin{array}{c} \rho \vdash e \downarrow \top \\ \rho \vdash s_1 \longrightarrow \rho'; O \end{array}}{\rho \vdash \mathbf{if}(e, s_1, s_2) \longrightarrow \rho'; O} \quad \text{SC\_IFT}$$

$$\frac{\begin{array}{c} \rho \vdash e \downarrow \bot \\ \rho \vdash s_2 \longrightarrow \rho'; O \end{array}}{\rho \vdash \mathbf{if}(e, s_1, s_2) \longrightarrow \rho'; O} \quad \text{SC\_IFF}$$

$$\frac{\rho \vdash e \downarrow v}{\rho \vdash \mathbf{out}\, e \longrightarrow \rho; v} \quad \text{SC\_OUT}$$

$$\frac{\begin{array}{c} \rho \vdash s_1 \longrightarrow \rho_1; O_1 \\ \rho_1 \vdash s_2 \longrightarrow \rho_2; O_2 \end{array}}{\rho \vdash s_1; s_2 \longrightarrow \rho_2; O_1, O_2} \quad \text{SC\_SEQ}$$

Figure 4: Source command evaluation

4

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

$$\frac{}{n : \mathsf{uint}^{\mathcal{P}}} \quad \text{V\_INT}$$

$$\frac{}{\top : \mathsf{bool}^{\mathcal{P}}} \quad \text{V\_TRUE}$$

$$\frac{}{\bot : \mathsf{bool}^{\mathcal{P}}} \quad \text{V\_FALSE}$$

$$\frac{c_i : \sigma}{[\,\overline{c_i}^{\,i}\,] : \sigma[\,]} \quad \text{V\_ARR}$$

Figure 5: Value typing

$\widetilde{e}$	::=		Target expression
	|	c	
	|	x	
	|	$\widetilde{e}_1 +_\ell \widetilde{e}_2$	
	|	$\mathbf{cond}_\ell(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2)$	
	|	$\widetilde{e}_1 >_\ell \widetilde{e}_2$	
	|	$x[\widetilde{e}]$	
	|	$\widetilde{e} \triangleright m$	

$\widetilde{s}$	::=		Target statement
	|	$\tau\, x$	
	|	$x := \widetilde{e}$	
	|	$\mathbf{for}(x := n_1; x \le n_2; x := x + 1)\, \widetilde{s}$	
	|	$x[\widetilde{e}_1] := \widetilde{e}_2$	
	|	$\mathbf{if}(\widetilde{e}, \widetilde{s}_1, \widetilde{s}_2)$	
	|	$\mathbf{out}\, \widetilde{e}$	
	|	$\widetilde{s}_1; \widetilde{s}_2$	
Γ	::=		Type environment
	|	$\cdot$	
	|	$\Gamma, x : \tau$	

Figure 6: Target language

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

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

$$\frac{}{\Gamma \vdash \top : \mathsf{bool}^{\mathcal{P}} \rightsquigarrow \top} \quad \text{S\_TRUE}$$

$$\frac{}{\Gamma \vdash \bot : \mathsf{bool}^{\mathcal{P}} \rightsquigarrow \bot} \quad \text{S\_FALSE}$$

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

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow \widetilde{e}_i}{\Gamma \vdash e_1 + e_2 : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow \widetilde{e}_1 +_{\mathcal{P}} \widetilde{e}_2} \quad \text{S\_PADD}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{A}} \rightsquigarrow \widetilde{e}_i}{\Gamma \vdash e_1 + e_2 : \mathsf{uint}^{\mathcal{A}} \rightsquigarrow \widetilde{e}_1 +_{\mathcal{A}} \widetilde{e}_2} \quad \text{S\_SADD}$$

$$\frac{\begin{array}{c}\Gamma \vdash e : \mathsf{bool}^{\mathcal{P}} \rightsquigarrow \widetilde{e} \\ \Gamma \vdash e_i : \sigma \rightsquigarrow \widetilde{e}_i\end{array}}{\Gamma \vdash \mathbf{cond}(e, e_1, e_2) : \sigma \rightsquigarrow \mathbf{cond}_{\mathcal{P}}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2)} \quad \text{S\_PCOND}$$

$$\frac{\begin{array}{c}\Gamma \vdash e : \mathsf{bool}^{\mathcal{B}} \rightsquigarrow \widetilde{e} \\ \Gamma \vdash e_i : \sigma \rightsquigarrow \widetilde{e}_i \\ \mathsf{label}(\sigma) = \mathcal{B}\end{array}}{\Gamma \vdash \mathbf{cond}(e, e_1, e_2) : \sigma \rightsquigarrow \mathbf{cond}_{\mathcal{B}}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2)} \quad \text{S\_SCOND}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow \widetilde{e}_i}{\Gamma \vdash e_1 > e_2 : \mathsf{bool}^{\mathcal{P}} \rightsquigarrow \widetilde{e}_1 >_{\mathcal{P}} \widetilde{e}_2} \quad \text{S\_PGT}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{B}} \rightsquigarrow \widetilde{e}_i}{\Gamma \vdash e_1 > e_2 : \mathsf{bool}^{\mathcal{B}} \rightsquigarrow \widetilde{e}_1 >_{\mathcal{B}} \widetilde{e}_2} \quad \text{S\_SGT}$$

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

$$\frac{\begin{array}{c}\Gamma \vdash e : \sigma_1 \rightsquigarrow \widetilde{e} \\ \mathsf{base}(\sigma_1) = \mathsf{base}(\sigma_2) \\ \mathsf{label}(\sigma_2) = m\end{array}}{\Gamma \vdash e : \sigma_2 \rightsquigarrow \widetilde{e} \triangleright m} \quad \text{S\_SUB}$$

Figure 7: Expression compilation

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

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

$$\frac{\begin{array}{c}\Gamma(x) = \sigma \\ \Gamma \vdash e : \sigma \rightsquigarrow \widetilde{e}\end{array}}{\Gamma \vdash x := e \rightsquigarrow x := \widetilde{e} \mid \Gamma}\ \text{C\_VASSGN}$$

$$\frac{\begin{array}{c}\Gamma, x : \mathsf{uint}^{\mathcal{P}} \vdash s \rightsquigarrow \widetilde{s} \mid \_ \\ x \notin \mathsf{modifies}(s)\end{array}}{\Gamma \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x+1)\ s \rightsquigarrow \mathbf{for}(x := n_1; x \leq n_2; x := x+1)\ \widetilde{s} \mid \Gamma}\ \text{C\_FOR}$$

$$\frac{\begin{array}{c}\Gamma \vdash x : \sigma[\,] \rightsquigarrow x \\ \Gamma \vdash e_1 : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow \widetilde{e}_1 \\ \Gamma \vdash e_2 : \sigma \rightsquigarrow \widetilde{e}_2\end{array}}{\Gamma \vdash x[e_1] := e_2 \rightsquigarrow x[\widetilde{e}_1] := \widetilde{e}_2 \mid \Gamma}\ \text{C\_AWRITE}$$

$$\frac{\begin{array}{c}\Gamma \vdash e : \mathsf{bool}^{\mathcal{P}} \rightsquigarrow \widetilde{e} \\ \Gamma \vdash s_i \rightsquigarrow \widetilde{s}_i \mid \_\end{array}}{\Gamma \vdash \mathbf{if}(e, s_1, s_2) \rightsquigarrow \mathbf{if}(\widetilde{e}, \widetilde{s}_1, \widetilde{s}_2) \mid \Gamma}\ \text{C\_IF}$$

$$\frac{\begin{array}{c}\Gamma \vdash e : \sigma \rightsquigarrow \widetilde{e} \\ \mathsf{label}(\sigma) = m\end{array}}{\Gamma \vdash \mathbf{out}\, e \rightsquigarrow \mathbf{out}\, \widetilde{e} \mid \Gamma}\ \text{C\_OUT}$$

$$\frac{\begin{array}{c}\Gamma \vdash s_1 \rightsquigarrow \widetilde{s}_1 \mid \Gamma_1 \\ \Gamma_1 \vdash s_2 \rightsquigarrow \widetilde{s}_2 \mid \Gamma'\end{array}}{\Gamma \vdash s_1; s_2 \rightsquigarrow \widetilde{s}_1; \widetilde{s}_2 \mid \Gamma'}\ \text{C\_SEQ}$$

Figure 8: Command compilation

$$
\begin{array}{llll}
r & ::= & & \text{Wire id range} \\[1.2em]
\widetilde{w} & ::= & & \text{Compiled base value} \\
& & |\quad c & \\
& & |\quad r & \\[1.2em]
\widetilde{v} & ::= & & \text{Compiled value} \\
& & |\quad \widetilde{w} & \\
& & |\quad [\,\overline{\widetilde{w}_i}^{\,i}\,] & \\[1.2em]
\kappa & ::= & & \text{Circuit} \\
& & |\quad \cdot & \\
& & |\quad \oplus(r_1, r_2, r_3) & \\
& & |\quad \mathsf{Mux}(r_1, r_2, r_3, r_4) & \\
& & |\quad \mathsf{Gt}(r_1, r_2, r_3) & \\
& & |\quad r_1 \rhd_m r_2 & \\
& & |\quad \mathsf{Out}(r) & \\
& & |\quad \kappa_1, \kappa_2 & \\[1.2em]
\widetilde{\rho} & ::= & & \text{Runtime environment} \\
& & |\quad \cdot & \\
& & |\quad \widetilde{\rho}[x \mapsto \widetilde{v}] &
\end{array}
$$

Figure 9: Target runtime

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

$$\frac{}{\widetilde{\rho} \vdash c \Downarrow c; \cdot} \quad \text{EE\_CONST}$$

$$\frac{}{\widetilde{\rho} \vdash x \Downarrow \widetilde{\rho}[x]; \cdot} \quad \text{EE\_VAR}$$

$$\frac{\widetilde{\rho} \vdash \widetilde{e}_i \Downarrow n_i; \kappa_i}{\widetilde{\rho} \vdash \widetilde{e}_1 +_{\mathcal{P}} \widetilde{e}_2 \Downarrow n_1 + n_2; \kappa_1, \kappa_2} \quad \text{EE\_PADD}$$

$$\frac{\begin{array}{c}\widetilde{\rho} \vdash \widetilde{e}_i \Downarrow r_i; \kappa_i \\ r_3 = \mathsf{next\_range}()\end{array}}{\widetilde{\rho} \vdash \widetilde{e}_1 +_{\mathcal{A}} \widetilde{e}_2 \Downarrow r_3; \kappa_1, \kappa_2, \oplus(r_1, r_2, r_3)} \quad \text{EE\_SADD}$$

$$\frac{\begin{array}{c}\widetilde{\rho} \vdash \widetilde{e} \Downarrow \top; \kappa \\ \widetilde{\rho} \vdash \widetilde{e}_1 \Downarrow \widetilde{v}; \kappa_1\end{array}}{\widetilde{\rho} \vdash \mathbf{cond}_{\mathcal{P}}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2) \Downarrow \widetilde{v}; \kappa, \kappa_1} \quad \text{EE\_PCONDT}$$

$$\frac{\begin{array}{c}\widetilde{\rho} \vdash \widetilde{e} \Downarrow \bot; \kappa \\ \widetilde{\rho} \vdash \widetilde{e}_2 \Downarrow \widetilde{v}; \kappa_2\end{array}}{\widetilde{\rho} \vdash \mathbf{cond}_{\mathcal{P}}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2) \Downarrow \widetilde{v}; \kappa, \kappa_2} \quad \text{EE\_PCONDF}$$

$$\frac{\begin{array}{c}\widetilde{\rho} \vdash \widetilde{e} \Downarrow r; \kappa \\ \widetilde{\rho} \vdash \widetilde{e}_i \Downarrow r_i; \kappa_i \\ r_3 = \mathsf{next\_range}()\end{array}}{\widetilde{\rho} \vdash \mathbf{cond}_{\mathcal{B}}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2) \Downarrow r_3; \kappa, \kappa_1, \kappa_2, \mathsf{Mux}(r, r_1, r_2, r_3)} \quad \text{EE\_SCOND}$$

$$\frac{\widetilde{\rho} \vdash \widetilde{e}_i \Downarrow n_i; \kappa_i}{\widetilde{\rho} \vdash \widetilde{e}_1 >_{\mathcal{P}} \widetilde{e}_2 \Downarrow n_1 > n_2; \kappa_1, \kappa_2} \quad \text{EE\_PGT}$$

$$\frac{\begin{array}{c}\widetilde{\rho} \vdash \widetilde{e}_i \Downarrow r_i; \kappa_i \\ r_3 = \mathsf{next\_range}()\end{array}}{\widetilde{\rho} \vdash \widetilde{e}_1 >_{\mathcal{B}} \widetilde{e}_2 \Downarrow r_3; \kappa_1, \kappa_2, \mathsf{Gt}(r_1, r_2, r_3)} \quad \text{EE\_SGT}$$

$$\frac{\begin{array}{c}\widetilde{\rho} \vdash \widetilde{e} \Downarrow n; \kappa_1 \\ \widetilde{\rho} \vdash x \Downarrow [\overline{\widetilde{w}_i}^i]; \kappa_2\end{array}}{\widetilde{\rho} \vdash x[\widetilde{e}] \Downarrow \widetilde{w}_n; \kappa_1, \kappa_2} \quad \text{EE\_AREAD}$$

$$\frac{\begin{array}{c}\widetilde{\rho} \vdash \widetilde{e} \Downarrow r; \kappa \\ r' = \mathsf{next\_range}()\end{array}}{\widetilde{\rho} \vdash \widetilde{e} \rhd m \Downarrow r'; \kappa, r \rhd_m r'} \quad \text{EE\_COERCE}$$

Figure 10: Target expression evaluation

9

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

$$\frac{\mathsf{default}(\tau) = \widetilde{v}; \kappa}{\widetilde{\rho} \vdash \tau\, x \Longrightarrow \widetilde{\rho}[x \mapsto \widetilde{v}]; \kappa} \quad \text{EC\_DECL}$$

$$\frac{\widetilde{\rho} \vdash \widetilde{e} \Downarrow \widetilde{v}; \kappa}{\widetilde{\rho} \vdash x := \widetilde{e} \Longrightarrow \widetilde{\rho}[x \mapsto \widetilde{v}]; \kappa} \quad \text{EC\_ASSGN}$$

$$\frac{n_1 > n_2}{\widetilde{\rho} \vdash \mathbf{for}(x := n_1; x \le n_2; x := x+1)\ \widetilde{s} \Longrightarrow \widetilde{\rho}; \cdot} \quad \text{EC\_FORT}$$

$$\frac{\begin{array}{l} n_2 \ge n_1 \\ \widetilde{\rho}[x \mapsto n_1] \vdash \widetilde{s} \Longrightarrow \widetilde{\rho}_1; \kappa_1 \\ \widetilde{\rho}_1 \vdash \mathbf{for}(x := n_1+1; x \le n_2; x := x+1)\ \widetilde{s} \Longrightarrow \widetilde{\rho}_2; \kappa_2 \end{array}}{\widetilde{\rho} \vdash \mathbf{for}(x := n_1; x \le n_2; x := x+1)\ \widetilde{s} \Longrightarrow \widetilde{\rho}_2; \kappa_1, \kappa_2} \quad \text{EC\_FORI}$$

$$\frac{\begin{array}{l} \widetilde{\rho} \vdash x \Downarrow [\,\overline{\widetilde{w}_i}^{\,i}\,]; \cdot \\ \widetilde{\rho} \vdash \widetilde{e}_1 \Downarrow n; \kappa_1 \\ \widetilde{\rho} \vdash \widetilde{e}_2 \Downarrow \widetilde{w}; \kappa_2 \end{array}}{\widetilde{\rho} \vdash x[\widetilde{e}_1] := \widetilde{e}_2 \Longrightarrow \widetilde{\rho}[x \mapsto [\,\overline{\widetilde{w}_i}^{\,i}\,][n \mapsto \widetilde{w}]]; \kappa_1, \kappa_2} \quad \text{EC\_AWRITE}$$

$$\frac{\begin{array}{l} \widetilde{\rho} \vdash \widetilde{e} \Downarrow \top; \kappa_1 \\ \widetilde{\rho} \vdash \widetilde{s}_1 \Longrightarrow \widetilde{\rho}'; \kappa_2 \end{array}}{\widetilde{\rho} \vdash \mathbf{if}(\widetilde{e}, \widetilde{s}_1, \widetilde{s}_2) \Longrightarrow \widetilde{\rho}'; \kappa_1, \kappa_2} \quad \text{EC\_IFT}$$

$$\frac{\begin{array}{l} \widetilde{\rho} \vdash \widetilde{e} \Downarrow \bot; \kappa_1 \\ \widetilde{\rho} \vdash \widetilde{s}_2 \Longrightarrow \widetilde{\rho}'; \kappa_2 \end{array}}{\widetilde{\rho} \vdash \mathbf{if}(\widetilde{e}, \widetilde{s}_1, \widetilde{s}_2) \Longrightarrow \widetilde{\rho}'; \kappa_1, \kappa_2} \quad \text{EC\_IFF}$$

$$\frac{\widetilde{\rho} \vdash \widetilde{e} \Downarrow r; \kappa}{\widetilde{\rho} \vdash \mathbf{out}\, \widetilde{e} \Longrightarrow \widetilde{\rho}; \kappa, \mathsf{Out}(r)} \quad \text{EC\_OUT}$$

$$\frac{\begin{array}{l} \widetilde{\rho} \vdash \widetilde{s}_1 \Longrightarrow \widetilde{\rho}_1; \kappa_1 \\ \widetilde{\rho}_1 \vdash \widetilde{s}_2 \Longrightarrow \widetilde{\rho}_2; \kappa_2 \end{array}}{\widetilde{\rho} \vdash \widetilde{s}_1; \widetilde{s}_2 \Longrightarrow \widetilde{\rho}_2; \kappa_1, \kappa_2} \quad \text{EC\_SEQ}$$
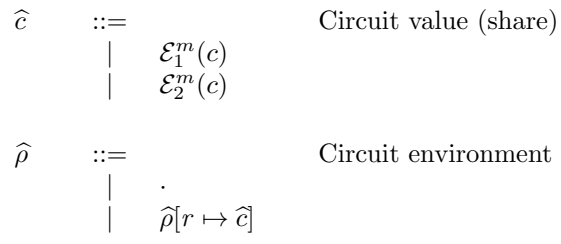
Figure 11: Target command evaluation

$$\widehat{c} \quad ::= \qquad\qquad\qquad \text{Circuit value (share)}$$
$$| \quad \mathcal{E}_1^m(c)$$
$$| \quad \mathcal{E}_2^m(c)$$

$$\widehat{\rho} \quad ::= \qquad\qquad\qquad \text{Circuit environment}$$
$$| \quad \cdot$$
$$| \quad \widehat{\rho}[r \mapsto \widehat{c}]$$

Figure 12: Circuit runtime

$$\boxed{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa \longmapsto \widehat{\rho}_1', \widehat{\rho}_2'; O}$$

$$\frac{}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \cdot \longmapsto \widehat{\rho}_1, \widehat{\rho}_2; \cdot} \quad \text{CKT\_EMP}$$

$$\frac{\widehat{\rho}_1[r_1] = \mathcal{E}_1^{\mathcal{A}}(n_1) \\ \widehat{\rho}_2[r_1] = \mathcal{E}_2^{\mathcal{A}}(n_1) \\ \widehat{\rho}_1[r_2] = \mathcal{E}_1^{\mathcal{A}}(n_2) \\ \widehat{\rho}_2[r_2] = \mathcal{E}_2^{\mathcal{A}}(n_2)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \oplus(r_1, r_2, r_3) \longmapsto \widehat{\rho}_1[r_3 \mapsto \mathcal{E}_1^{\mathcal{A}}((n_1 + n_2))], \widehat{\rho}_2[r_3 \mapsto \mathcal{E}_2^{\mathcal{A}}((n_1 + n_2))]; \cdot} \quad \text{CKT\_ADD}$$

$$\frac{\widehat{\rho}_1[r_1] = \mathcal{E}_1^{\mathcal{B}}(\top) \\ \widehat{\rho}_2[r_1] = \mathcal{E}_2^{\mathcal{B}}(\top) \\ \widehat{\rho}_1[r_2] = \mathcal{E}_1^{\mathcal{B}}(c) \\ \widehat{\rho}_2[r_2] = \mathcal{E}_2^{\mathcal{B}}(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Mux}(r_1, r_2, r_3, r_4) \longmapsto \widehat{\rho}_1[r_4 \mapsto \mathcal{E}_1^{\mathcal{B}}(c)], \widehat{\rho}_2[r_4 \mapsto \mathcal{E}_2^{\mathcal{B}}(c)]; \cdot} \quad \text{CKT\_MUXT}$$

$$\frac{\widehat{\rho}_1[r_1] = \mathcal{E}_1^{\mathcal{B}}(\bot) \\ \widehat{\rho}_2[r_1] = \mathcal{E}_2^{\mathcal{B}}(\bot) \\ \widehat{\rho}_1[r_3] = \mathcal{E}_1^{\mathcal{B}}(c) \\ \widehat{\rho}_2[r_3] = \mathcal{E}_2^{\mathcal{B}}(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Mux}(r_1, r_2, r_3, r_4) \longmapsto \widehat{\rho}_1[r_4 \mapsto \mathcal{E}_1^{\mathcal{B}}(c)], \widehat{\rho}_2[r_4 \mapsto \mathcal{E}_2^{\mathcal{B}}(c)]; \cdot} \quad \text{CKT\_MUXF}$$

$$\frac{\widehat{\rho}_1[r_1] = \mathcal{E}_1^{\mathcal{B}}(n_1) \\ \widehat{\rho}_2[r_1] = \mathcal{E}_2^{\mathcal{B}}(n_1) \\ \widehat{\rho}_1[r_2] = \mathcal{E}_1^{\mathcal{B}}(n_2) \\ \widehat{\rho}_2[r_2] = \mathcal{E}_2^{\mathcal{B}}(n_2) \\ c = n_1 > n_2}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Gt}(r_1, r_2, r_3) \longmapsto \widehat{\rho}_1[r_3 \mapsto \mathcal{E}_1^{\mathcal{B}}(c)], \widehat{\rho}_2[r_3 \mapsto \mathcal{E}_2^{\mathcal{B}}(c)]; \cdot} \quad \text{CKT\_GT}$$

$$\frac{\widehat{\rho}_1[r_1] = \mathcal{E}_1^{m_1}(c) \\ \widehat{\rho}_2[r_1] = \mathcal{E}_2^{m_1}(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash r_1 \rhd_m r_2 \longmapsto \widehat{\rho}_1[r_2 \mapsto \mathcal{E}_1^m(c)], \widehat{\rho}_2[r_2 \mapsto \mathcal{E}_2^m(c)]; \cdot} \quad \text{CKT\_COERCE}$$

$$\frac{\widehat{\rho}_1[r] = \mathcal{E}_1^m(c) \\ \widehat{\rho}_2[r] = \mathcal{E}_2^m(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Out}(r) \longmapsto \widehat{\rho}_1, \widehat{\rho}_2; c} \quad \text{CKT\_OUT}$$

$$\frac{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1 \longmapsto \widehat{\rho}_1', \widehat{\rho}_2'; O_1 \\ \widehat{\rho}_1', \widehat{\rho}_2' \vdash \kappa_2 \longmapsto \widehat{\rho}_1'', \widehat{\rho}_2''; O_2}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1, \kappa_2 \longmapsto \widehat{\rho}_1'', \widehat{\rho}_2''; O_1, O_2} \quad \text{CKT\_SEQ}$$

Figure 13: Circuit evaluation

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

$$\frac{}{\cdot \sim \cdot} \quad \text{SEN\_EMP}$$

$$\frac{\begin{array}{c} v : [\tau]_{\mathcal{P}} \\ \Gamma \sim \rho \end{array}}{\Gamma, x : \tau \sim \rho[x \mapsto v]} \quad \text{SEN\_BND}$$

Figure 14: Source environment and type environment consistency

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

$$\frac{}{\Gamma \vdash \cdot \hookrightarrow \cdot} \quad \text{TEN\_EMP}$$

$$\frac{\begin{array}{c} \Gamma(x) = \mathsf{uint}^{\mathcal{P}} \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho} \end{array}}{\Gamma \vdash \rho[x \mapsto n] \hookrightarrow \widetilde{\rho}[x \mapsto n]} \quad \text{TEN\_PINT}$$

$$\frac{\begin{array}{c} \Gamma(x) = \mathsf{uint}^{m} \\ r = \mathsf{next\_range}() \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho} \end{array}}{\Gamma \vdash \rho[x \mapsto n] \hookrightarrow \widetilde{\rho}[x \mapsto r]} \quad \text{TEN\_SINT}$$

$$\frac{\begin{array}{c} \Gamma(x) = \mathsf{bool}^{\mathcal{P}} \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho} \end{array}}{\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \widetilde{\rho}[x \mapsto c]} \quad \text{TEN\_PBOOL}$$

$$\frac{\begin{array}{c} \Gamma(x) = \mathsf{bool}^{m} \\ r = \mathsf{next\_range}() \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho} \end{array}}{\Gamma \vdash \rho[x \mapsto \_] \hookrightarrow \widetilde{\rho}[x \mapsto r]} \quad \text{TEN\_SBOOL}$$

$$\frac{\begin{array}{c} \Gamma(x) = \sigma[\,] \\ \mathsf{label}(\sigma) = \mathcal{P} \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho} \end{array}}{\Gamma \vdash \rho[x \mapsto [\overline{c_i}^{\,i}]] \hookrightarrow \widetilde{\rho}[x \mapsto [\overline{c_i}^{\,i}]]} \quad \text{TEN\_PARR}$$

$$\frac{\begin{array}{c} \Gamma(x) = \sigma[\,] \\ \mathsf{label}(\sigma) = m \\ r_i = \mathsf{next\_range}() \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho} \end{array}}{\Gamma \vdash \rho[x \mapsto [\overline{c_i}^{\,i}]] \hookrightarrow \widetilde{\rho}[x \mapsto [\overline{r_i}^{\,i}]]} \quad \text{TEN\_SARR}$$

Figure 15: Source environment to target environment compilation

$$\boxed{\Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2}$$

$$\frac{}{\Gamma; \widetilde{\rho} \vdash \cdot \hookrightarrow \cdot, \cdot} \quad \text{CEN\_EMP}$$

$$\frac{\Gamma(x) = \mathsf{uint}^{\mathcal{P}} \quad \Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2}{\Gamma; \widetilde{\rho} \vdash \rho[x \mapsto n] \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2} \quad \text{CEN\_PINT}$$

$$\frac{\Gamma(x) = \mathsf{uint}^{m} \quad \widetilde{\rho}[x] = r \quad \Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2}{\Gamma; \widetilde{\rho} \vdash \rho[x \mapsto n] \hookrightarrow \widehat{\rho}_1[r \mapsto \mathcal{E}_1^m(n)], \widehat{\rho}_2[r \mapsto \mathcal{E}_2^m(n)]} \quad \text{CEN\_SINT}$$

$$\frac{\Gamma(x) = \mathsf{bool}^{\mathcal{P}} \quad \Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2}{\Gamma; \widetilde{\rho} \vdash \rho[x \mapsto c] \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2} \quad \text{CEN\_PBOOL}$$

$$\frac{\Gamma(x) = \mathsf{bool}^{m} \quad \widetilde{\rho}[x] = r \quad \Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2}{\Gamma; \widetilde{\rho} \vdash \rho[x \mapsto c] \hookrightarrow \widehat{\rho}_1[r \mapsto \mathcal{E}_1^m(c)], \widehat{\rho}_2[r \mapsto \mathcal{E}_2^m(c)]} \quad \text{CEN\_SBOOL}$$

$$\frac{\Gamma(x) = \sigma[\,] \quad \mathsf{label}(\sigma) = \mathcal{P} \quad \Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2}{\Gamma; \widetilde{\rho} \vdash \rho[x \mapsto [\,\overline{c_i}^{\,i}\,]] \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2} \quad \text{CEN\_PARR}$$

$$\frac{\Gamma(x) = \sigma[\,] \quad \mathsf{label}(\sigma) = m \quad \widetilde{\rho}[x] = [\,\overline{r_i}^{\,i}\,] \quad \Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2}{\Gamma; \widetilde{\rho} \vdash \rho[x \mapsto [\,\overline{c_i}^{\,i}\,]] \hookrightarrow \widehat{\rho}_1[r_i \mapsto \mathcal{E}_1^m(c_i)], \widehat{\rho}_2[r_i \mapsto \mathcal{E}_2^m(c_i)]} \quad \text{CEN\_SARR}$$

Figure 16: Source environment to circuit environment compilation