

$\sigma ::=$	Base type
	uint
	bool
$\psi ::=$	Source type
	$\sigma$
	$\sigma[n]$
$c ::=$	Constant
	$n$
	$\top$
	$\perp$
$e ::=$	Source expression
	$c$
	$x$
	$e_1 + e_2$
	<b>cond</b> ( $e, e_1, e_2$ )
	$e_1 > e_2$
	$[e_i]_n$
	$x[e]$
	<b>in</b> <sub><math>j</math></sub>
$s ::=$	Source statement
	$\psi \ x = e$
	$x := e$
	<b>for</b> $x$ <b>in</b> $n_1 \dots n_2$ <b>do</b> $s$
	$x[e_1] := e_2$
	<b>if</b> ( $e, s_1, s_2$ )
	<b>out</b> $e$
	$s_1; s_2$

Figure 1: Source language

$v ::=$	Source value
	$c$
	$[c_i]_n$
$\rho ::=$	Source runtime environment
	$\cdot$
	$\rho[x \mapsto v]$
$O ::=$	Source observation
	$\cdot$
	$c, O$

Figure 2: Source runtime

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

$$\begin{array}{c}
\frac{}{\rho \vdash c \Downarrow c} \text{ SE\_CONST} \\
\\
\frac{}{\rho \vdash x \Downarrow \rho(x)} \text{ SE\_VAR} \\
\\
\frac{\forall i \in \{1, 2\}. \rho \vdash e_i \Downarrow n_i}{\rho \vdash e_1 + e_2 \Downarrow n_1 + n_2} \text{ SE\_ADD} \\
\\
\frac{\begin{array}{l} \rho \vdash e \Downarrow c \\ c = \top \Rightarrow i = 1 \\ c = \perp \Rightarrow i = 2 \\ \rho \vdash e_i \Downarrow v \end{array}}{\rho \vdash \mathbf{cond}(e, e_1, e_2) \Downarrow v} \text{ SE\_COND} \\
\\
\frac{\forall i \in \{1, 2\}. \rho \vdash e_i \Downarrow n_i}{\rho \vdash e_1 > e_2 \Downarrow n_1 > n_2} \text{ SE\_GT} \\
\\
\frac{\forall i \in \{0, n-1\}. \rho \vdash e_i \Downarrow c_i}{\rho \vdash [e_i]_n \Downarrow [c_i]_n} \text{ SE\_ARR} \\
\\
\frac{\begin{array}{l} \rho \vdash x \Downarrow [c_i]_{n'} \\ \rho \vdash e \Downarrow n \\ n < n' \end{array}}{\rho \vdash x[e] \Downarrow c_n} \text{ SE\_AREAD} \\
\\
\frac{}{\rho \vdash \mathbf{in}_j \Downarrow c} \text{ SE\_INP}
\end{array}$$

Figure 3: Source expression evaluation

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

$$\begin{array}{c}
\frac{\rho \vdash e \Downarrow v}{\rho \vdash \psi \ x = e \Downarrow \rho[x \mapsto v]; \cdot} \quad \text{SC\_DECL} \\
\\
\frac{\rho \vdash e \Downarrow v}{\rho \vdash x := e \Downarrow \rho[x \mapsto v]; \cdot} \quad \text{SC\_ASSGN} \\
\\
\frac{\rho[x \mapsto n_1] \vdash \text{loop } x \text{ until } n_2 \text{ do } s \Downarrow \rho_1; O}{\rho \vdash \text{for } x \text{ in } n_1 \dots n_2 \text{ do } s \Downarrow \rho_1 \setminus x; O} \quad \text{SC\_FORT} \\
\\
\frac{\rho(x) > n_2}{\rho \vdash \text{loop } x \text{ until } n_2 \text{ do } s \Downarrow \rho; O} \quad \text{SC\_LOOP} \\
\\
\frac{\begin{array}{l} \rho(x) \leq n_2 \\ \rho \vdash s \Downarrow \rho_1; O_1 \\ ([\rho_1]_{\text{dom}(\rho)})(x \mapsto \rho(x) + 1) \vdash \text{loop } x \text{ until } n_2 \text{ do } s \Downarrow \rho_2; O_2 \end{array}}{\rho \vdash \text{loop } x \text{ until } n_2 \text{ do } s \Downarrow \rho_2; O_1, O_2} \quad \text{SC\_LOOPI} \\
\\
\frac{\begin{array}{l} \rho \vdash x \Downarrow [c_i]_{n'} \\ \rho \vdash e_1 \Downarrow n \\ \rho \vdash e_2 \Downarrow c \\ n < n' \end{array}}{\rho \vdash x[e_1] := e_2 \Downarrow \rho[x \mapsto [c_i]_{n'}[n \mapsto c]]; \cdot} \quad \text{SC\_AWRITE} \\
\\
\frac{\begin{array}{l} \rho \vdash e \Downarrow c \\ c = \top \Rightarrow i = 1 \\ c = \perp \Rightarrow i = 2 \\ \rho \vdash s_i \Downarrow \rho'; O \end{array}}{\rho \vdash \text{if}(e, s_1, s_2) \Downarrow \rho'; O} \quad \text{SC\_IF} \\
\\
\frac{\rho \vdash e \Downarrow c}{\rho \vdash \text{out } e \Downarrow \rho; c, \cdot} \quad \text{SC\_OUT} \\
\\
\frac{\begin{array}{l} \rho \vdash s_1 \Downarrow \rho_1; O_1 \\ \rho_1 \vdash s_2 \Downarrow \rho_2; O_2 \end{array}}{\rho \vdash s_1; s_2 \Downarrow \rho_2; O_1, O_2} \quad \text{SC\_SEQ}
\end{array}$$

Figure 4: Source command evaluation

$$\boxed{v : \psi}$$

$$\begin{array}{c}
\frac{}{c : \text{typeof}(c)} \quad \text{V\_CONS} \\
\\
\frac{\forall i \in \{0, n-1\}. c_i : \sigma}{[c_i]_n : \sigma[n]} \quad \text{V\_ARR}
\end{array}$$

Figure 5: Value typing

$m ::=$	$\mathcal{A}$ $\mathcal{B}$	Secret label
$\ell ::=$	$\mathcal{P}$ $m$	Label
$\tau ::=$	$\sigma^\ell$ $\sigma^\ell[n]$	Type
$\tilde{e} ::=$	$c$ $x$ $\tilde{e}_1 +_\ell \tilde{e}_2$ $\mathbf{cond}_\ell(\tilde{e}, \tilde{e}_1, \tilde{e}_2)$ $\tilde{e}_1 >_\ell \tilde{e}_2$ $[e_i]_n$ $x[\tilde{e}]$ $\mathbf{in}_j^m$ $\tilde{e} \triangleright m$	Target expression
$\tilde{s} ::=$	$\tau x = \tilde{e}$ $x := \tilde{e}$ $\mathbf{for}(x := n_1; x \leq n_2; x := x + 1) \tilde{s}$ $x[\tilde{e}_1] := \tilde{e}_2$ $\mathbf{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2)$ $\mathbf{out} \tilde{e}$ $\tilde{s}_1; \tilde{s}_2$	Target statement
$\Gamma ::=$	$\cdot$ $\Gamma, x : \tau$	Type environment

Figure 6: Target language

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

$$\begin{array}{c}
\overline{\Gamma \vdash c : \text{typeof}(c)^{\mathcal{P}} \rightsquigarrow c} \quad \text{S\_CONS} \\
\\
\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau \rightsquigarrow x} \quad \text{S\_VAR} \\
\\
\frac{\begin{array}{l} \forall i \in \{1, 2\}. \Gamma \vdash e_i : \text{uint}^\ell \rightsquigarrow \tilde{e}_i \\ \ell = \mathcal{P} \vee \ell = \mathcal{A} \end{array}}{\Gamma \vdash e_1 + e_2 : \text{uint}^\ell \rightsquigarrow \tilde{e}_1 +_\ell \tilde{e}_2} \quad \text{S\_ADD} \\
\\
\frac{\begin{array}{l} \Gamma \vdash e : \text{bool}^\ell \rightsquigarrow \tilde{e} \\ \forall i \in \{1, 2\}. \Gamma \vdash e_i : \sigma^{\ell'} \rightsquigarrow \tilde{e}_i \\ \ell = \mathcal{P} \vee (\ell = \mathcal{B} \wedge \ell' = \mathcal{B}) \end{array}}{\Gamma \vdash \mathbf{cond}(e, e_1, e_2) : \sigma^{\ell'} \rightsquigarrow \mathbf{cond}_\ell(\tilde{e}, \tilde{e}_1, \tilde{e}_2)} \quad \text{S\_COND} \\
\\
\frac{\begin{array}{l} \forall i \in \{1, 2\}. \Gamma \vdash e_i : \text{uint}^\ell \rightsquigarrow \tilde{e}_i \\ \ell = \mathcal{P} \vee \ell = \mathcal{B} \end{array}}{\Gamma \vdash e_1 > e_2 : \text{bool}^\ell \rightsquigarrow \tilde{e}_1 >_\ell \tilde{e}_2} \quad \text{S\_GT} \\
\\
\frac{\forall i \in \{0, n-1\}. \Gamma \vdash e_i : \sigma^\ell \rightsquigarrow \tilde{e}_i}{\Gamma \vdash [e_i]_n : \sigma^\ell[n] \rightsquigarrow [\tilde{e}_i]_n} \quad \text{S\_ARR} \\
\\
\frac{\begin{array}{l} \Gamma \vdash x : \sigma^\ell[n] \rightsquigarrow x \\ \Gamma \vdash e : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e} \\ \Gamma \models e < n \end{array}}{\Gamma \vdash x[e] : \sigma^\ell \rightsquigarrow x[\tilde{e}]} \quad \text{S\_AREAD} \\
\\
\overline{\Gamma \vdash \mathbf{in}_j : \sigma^m \rightsquigarrow \mathbf{in}_j^m} \quad \text{S\_INP} \\
\\
\frac{\Gamma \vdash e : \sigma^\ell \rightsquigarrow \tilde{e}}{\Gamma \vdash e : \sigma^m \rightsquigarrow \tilde{e} \triangleright m} \quad \text{S\_SUB}
\end{array}$$

Figure 7: Expression compilation

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

$$\frac{
\begin{array}{l}
\psi = \sigma \Rightarrow \tau = \sigma^\ell \\
\psi = \sigma[n] \Rightarrow \tau = \sigma^\ell[n] \\
\Gamma \vdash e : \tau \rightsquigarrow \tilde{e}
\end{array}
}{\Gamma \vdash \psi x = e \rightsquigarrow \tau x = \tilde{e} \mid \Gamma, x : \tau} \text{C\_DECL}$$

$$\frac{
\begin{array}{l}
\Gamma(x) = \sigma^\ell \\
\Gamma \vdash e : \sigma^\ell \rightsquigarrow \tilde{e}
\end{array}
}{\Gamma \vdash x := e \rightsquigarrow x := \tilde{e} \mid \Gamma} \text{C\_VASSGN}$$

$$\frac{
\begin{array}{l}
\Gamma, x : \text{uint}^{\mathcal{P}} \vdash s \rightsquigarrow \tilde{s} \mid - \\
x \notin \text{modifies}(s)
\end{array}
}{\Gamma \vdash \text{for } x \text{ in } n_1 \dots n_2 \text{ do } s \rightsquigarrow \text{for}(x := n_1; x \leq n_2; x := x + 1) \tilde{s} \mid \Gamma} \text{C\_FOR}$$

$$\frac{
\begin{array}{l}
\Gamma \vdash x : \sigma^\ell[n] \rightsquigarrow x \\
\Gamma \vdash e_1 : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}_1 \\
\Gamma \vdash e_2 : \sigma^\ell \rightsquigarrow \tilde{e}_2 \\
\Gamma \models e_1 < n
\end{array}
}{\Gamma \vdash x[e_1] := e_2 \rightsquigarrow x[\tilde{e}_1] := \tilde{e}_2 \mid \Gamma} \text{C\_AWRITE}$$

$$\frac{
\begin{array}{l}
\Gamma \vdash e : \text{bool}^{\mathcal{P}} \rightsquigarrow \tilde{e} \\
\forall i \in \{1, 2\}. \Gamma \vdash s_i \rightsquigarrow \tilde{s}_i \mid -
\end{array}
}{\Gamma \vdash \text{if}(e, s_1, s_2) \rightsquigarrow \text{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2) \mid \Gamma} \text{C\_IF}$$

$$\frac{\Gamma \vdash e : \sigma^m \rightsquigarrow \tilde{e}}{\Gamma \vdash \text{out } e \rightsquigarrow \text{out } \tilde{e} \mid \Gamma} \text{C\_OUT}$$

$$\frac{
\begin{array}{l}
\Gamma \vdash s_1 \rightsquigarrow \tilde{s}_1 \mid \Gamma_1 \\
\Gamma_1 \vdash s_2 \rightsquigarrow \tilde{s}_2 \mid \Gamma_2
\end{array}
}{\Gamma \vdash s_1; s_2 \rightsquigarrow \tilde{s}_1; \tilde{s}_2 \mid \Gamma_2} \text{C\_SEQ}$$

Figure 8: Command compilation

$r$	$::=$	Wire id range
$\kappa^e$	$::=$	Circuit expression
	$ $	
	$r$	
	$\text{In}_j^m$	
	$\text{Add}(\kappa_1^e, \kappa_2^e)$	
	$\text{Gt}(\kappa_1^e, \kappa_2^e)$	
	$\text{Mux}(\kappa^e, \kappa_1^e, \kappa_2^e)$	
	$\hat{w} \triangleright m$	
$\hat{w}$	$::=$	Compiled base value
	$ $	
	$c$	
	$\kappa^e$	
$\tilde{v}$	$::=$	Compiled value
	$ $	
	$\hat{w}$	
	$[\tilde{w}_i]_n$	
$\tilde{\rho}$	$::=$	Runtime environment
	$ $	
	$\cdot$	
	$\tilde{\rho}[x \mapsto \tilde{v}]$	
$\kappa^s$	$::=$	Circuit command
	$ $	
	$\cdot$	
	$\text{Bind}(\kappa^e, r)$	
	$\text{Out } \kappa^e$	
	$\kappa_1^s, \kappa_2^s$	

Figure 9: Target runtime

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

$$\begin{array}{c}
\frac{}{\tilde{\rho} \vdash c \Downarrow c} \text{EE\_CONST} \\
\\
\frac{}{\tilde{\rho} \vdash x \Downarrow \tilde{\rho}(x)} \text{EE\_VAR} \\
\\
\frac{\forall i \in \{1, 2\}. \tilde{\rho} \vdash \tilde{e}_i \Downarrow n_i}{\tilde{\rho} \vdash \tilde{e}_1 +_{\mathcal{P}} \tilde{e}_2 \Downarrow n_1 + n_2} \text{EE\_PADD} \\
\\
\frac{\forall i \in \{1, 2\}. \tilde{\rho} \vdash \tilde{e}_i \Downarrow \kappa_i^e}{\tilde{\rho} \vdash \tilde{e}_1 +_{\mathcal{A}} \tilde{e}_2 \Downarrow \text{Add}(\kappa_1^e, \kappa_2^e)} \text{EE\_SADD} \\
\\
\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{e} \Downarrow c \\ c = \top \Rightarrow i = 1 \\ c = \perp \Rightarrow i = 2 \\ \tilde{\rho} \vdash \tilde{e}_i \Downarrow \tilde{v} \end{array}}{\tilde{\rho} \vdash \mathbf{cond}_{\mathcal{P}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2) \Downarrow \tilde{v}} \text{EE\_PCOND} \\
\\
\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{e} \Downarrow \kappa^e \\ \forall i \in \{1, 2\}. \tilde{\rho} \vdash \tilde{e}_i \Downarrow \kappa_i^e \end{array}}{\tilde{\rho} \vdash \mathbf{cond}_{\mathcal{B}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2) \Downarrow \text{Mux}(\kappa^e, \kappa_1^e, \kappa_2^e)} \text{EE\_SCOND} \\
\\
\frac{\forall i \in \{1, 2\}. \tilde{\rho} \vdash \tilde{e}_i \Downarrow n_i}{\tilde{\rho} \vdash \tilde{e}_1 >_{\mathcal{P}} \tilde{e}_2 \Downarrow n_1 > n_2} \text{EE\_PGT} \\
\\
\frac{\forall i \in \{1, 2\}. \tilde{\rho} \vdash \tilde{e}_i \Downarrow \kappa_i^e}{\tilde{\rho} \vdash \tilde{e}_1 >_{\mathcal{B}} \tilde{e}_2 \Downarrow \text{Gt}(\kappa_1^e, \kappa_2^e)} \text{EE\_SGT} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e}_i \Downarrow \tilde{w}_i}{\tilde{\rho} \vdash [\tilde{e}_i]_n \Downarrow [\tilde{w}_i]_n} \text{EE\_ARR} \\
\\
\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{e} \Downarrow n \\ \tilde{\rho} \vdash x \Downarrow [\tilde{w}_i]_{n'} \\ n < n' \end{array}}{\tilde{\rho} \vdash x[\tilde{e}] \Downarrow \tilde{w}_n} \text{EE\_AREAD} \\
\\
\frac{}{\tilde{\rho} \vdash \mathbf{in}_j^m \Downarrow \mathbf{ln}_j^m} \text{EE\_INP} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow \tilde{w}}{\tilde{\rho} \vdash \tilde{e} \triangleright m \Downarrow \tilde{w} \triangleright m} \text{EE\_COERCE}
\end{array}$$

Figure 10: Target expression evaluation



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

$$\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow \tilde{v} \quad \tilde{v} = c \vee \tilde{v} = [c_i]_n}{\tilde{\rho} \vdash \tau x = \tilde{e} \Downarrow \tilde{\rho}[x \mapsto \tilde{v}]; \cdot} \text{EC\_DECL}$$

$$\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow \kappa^e \quad r = \text{next\_range}()}{\tilde{\rho} \vdash \tau x = \tilde{e} \Downarrow \tilde{\rho}[x \mapsto r]; \text{Bind}(\kappa^e, r)} \text{EC\_DECLCKT}$$

$$\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow [\kappa_i^e]_n \quad \forall i \in \{0, n-1\}. r_i = \text{next\_range}()}{\tilde{\rho} \vdash \tau x = \tilde{e} \Downarrow \tilde{\rho}[x \mapsto [r_i]_n]; \text{Bind}(\kappa_i^e, r_i)} \text{EC\_DECLCKTARR}$$

$$\frac{\tilde{\rho}[x \mapsto n_1] \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \mathbf{do} \ \tilde{s} \Downarrow \tilde{\rho}_1; \kappa^s}{\tilde{\rho} \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) \ \tilde{s} \Downarrow \tilde{\rho}_1 \setminus x; \kappa^s} \text{EC\_FORT}$$

$$\frac{\tilde{\rho}(x) > n_2}{\tilde{\rho} \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \mathbf{do} \ \tilde{s} \Downarrow \tilde{\rho}; \cdot} \text{EC\_LOOP}$$

$$\frac{\begin{array}{l} \tilde{\rho}(x) \leq n_2 \\ \tilde{\rho} \vdash \tilde{s} \Downarrow \tilde{\rho}_1; \kappa_1^s \\ ([\tilde{\rho}_1]_{\text{dom}(\tilde{\rho})})[x \mapsto \tilde{\rho}(x) + 1] \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \mathbf{do} \ \tilde{s} \Downarrow \tilde{\rho}_2; \kappa_2^s \end{array}}{\tilde{\rho} \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \mathbf{do} \ \tilde{s} \Downarrow \tilde{\rho}_2; \kappa_1^s, \kappa_2^s} \text{EC\_LOOPI}$$

$$\frac{\begin{array}{l} \tilde{\rho} \vdash x \Downarrow [\tilde{w}_i]_{n'} \\ \tilde{\rho} \vdash \tilde{e}_1 \Downarrow n \\ \tilde{\rho} \vdash \tilde{e}_2 \Downarrow \tilde{w} \\ n < n' \end{array}}{\tilde{\rho} \vdash x[\tilde{e}_1] := \tilde{e}_2 \Downarrow \tilde{\rho}[x \mapsto [\tilde{w}_i]_{n'}[n \mapsto \tilde{w}]]; \cdot} \text{EC\_AWRITE}$$

$$\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{e} \Downarrow c \\ c = \top \Rightarrow i = 1 \\ c = \perp \Rightarrow i = 2 \\ \tilde{\rho} \vdash \tilde{s}_i \Downarrow \tilde{\rho}'; \kappa^s \end{array}}{\tilde{\rho} \vdash \mathbf{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2) \Downarrow \tilde{\rho}'; \kappa^s} \text{EC\_IF}$$

$$\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow \kappa^e}{\tilde{\rho} \vdash \mathbf{out} \ \tilde{e} \Downarrow \tilde{\rho}; \text{Out} \ \kappa^e} \text{EC\_OUT}$$

$$\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{s}_1 \Downarrow \tilde{\rho}_1; \kappa_1^s \\ \tilde{\rho}_1 \vdash \tilde{s}_2 \Downarrow \tilde{\rho}_2; \kappa_2^s \end{array}}{\tilde{\rho} \vdash \tilde{s}_1; \tilde{s}_2 \Downarrow \tilde{\rho}_2; \kappa_1^s, \kappa_2^s} \text{EC\_SEQ}$$

Figure 11: Target command evaluation

$b ::=$  Share (byte string)  
 $\hat{\rho} ::=$  Circuit environment  
 $\quad \mid \cdot$   
 $\quad \mid \hat{\rho}[r \mapsto b]$

Figure 12: Circuit runtime

$$\boxed{\hat{\rho}_1, \hat{\rho}_2 \vdash \kappa^e \Downarrow b_1, b_2}$$

$$\begin{array}{c}
\frac{}{\hat{\rho}_1, \hat{\rho}_2 \vdash r \Downarrow \hat{\rho}_1[r], \hat{\rho}_2[r]} \text{CKTE\_R} \\
\\
\frac{(b_1, b_2) = \mathcal{E}_m(c)}{\hat{\rho}_1, \hat{\rho}_2 \vdash \text{In}_j^m \Downarrow b_1, b_2} \text{CKTE\_IN} \\
\\
\frac{\begin{array}{l} \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa_1^e \Downarrow b_{11}, b_{21} \\ \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa_2^e \Downarrow b_{12}, b_{22} \\ n_1 = \mathcal{D}_{\mathcal{A}}(b_{11}, b_{21}) \\ n_2 = \mathcal{D}_{\mathcal{A}}(b_{12}, b_{22}) \\ (b_1, b_2) = \mathcal{E}_{\mathcal{A}}(n_1 + n_2) \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \text{Add}(\kappa_1^e, \kappa_2^e) \Downarrow b_1, b_2} \text{CKTE\_ADD} \\
\\
\frac{\begin{array}{l} \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa_1^e \Downarrow b_{11}, b_{21} \\ \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa_2^e \Downarrow b_{12}, b_{22} \\ n_1 = \mathcal{D}_{\mathcal{B}}(b_{11}, b_{21}) \\ n_2 = \mathcal{D}_{\mathcal{B}}(b_{12}, b_{22}) \\ (b_1, b_2) = \mathcal{E}_{\mathcal{B}}(n_1 > n_2) \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \text{Gt}(\kappa_1^e, \kappa_2^e) \Downarrow b_1, b_2} \text{CKTE\_GT} \\
\\
\frac{\begin{array}{l} \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa^e \Downarrow b_1, b_2 \\ \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa_1^e \Downarrow b_{11}, b_{21} \\ \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa_2^e \Downarrow b_{12}, b_{22} \\ c = \mathcal{D}_{\mathcal{B}}(b_1, b_2) \\ c_1 = \mathcal{D}_{\mathcal{B}}(b_{11}, b_{21}) \\ c_2 = \mathcal{D}_{\mathcal{B}}(b_{12}, b_{22}) \\ c = \top \Rightarrow (b'_1, b'_2) = \mathcal{E}_{\mathcal{B}}(c_1) \\ c = \perp \Rightarrow (b'_1, b'_2) = \mathcal{E}_{\mathcal{B}}(c_2) \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \text{Mux}(\kappa^e, \kappa_1^e, \kappa_2^e) \Downarrow b'_1, b'_2} \text{CKTE\_MUX} \\
\\
\frac{(b_1, b_2) = \mathcal{E}_m(c)}{\hat{\rho}_1, \hat{\rho}_2 \vdash c \triangleright m \Downarrow b_1, b_2} \text{CKTE\_COERCEC} \\
\\
\frac{\begin{array}{l} \hat{\rho}_1, \hat{\rho}_2 \vdash \kappa^e \Downarrow b_1, b_2 \\ c = \mathcal{D}_{m_1}(b_1, b_2) \\ (b'_1, b'_2) = \mathcal{E}_m(c) \end{array}}{\hat{\rho}_1, \hat{\rho}_2 \vdash \kappa^e \triangleright m \Downarrow b'_1, b'_2} \text{CKTE\_COERCER}
\end{array}$$

Figure 13: Circuit expression evaluation

$$\boxed{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa^s \Downarrow \widetilde{\rho}'_1, \widetilde{\rho}'_2; O}$$

$$\begin{array}{c}
\frac{}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \cdot \Downarrow \widehat{\rho}_1, \widehat{\rho}_2; \cdot} \text{CKTC\_EMP} \\
\frac{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa^e \Downarrow b_1, b_2}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \text{Bind}(\kappa^e, r) \Downarrow \widehat{\rho}_1[r \mapsto b_1], \widehat{\rho}_2[r \mapsto b_1]; \cdot} \text{CKTC\_BIND} \\
\frac{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa^e \Downarrow b_1, b_2 \quad c = \mathcal{D}_m(b_1, b_2)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \text{Out } \kappa^e \Downarrow \widehat{\rho}_1, \widehat{\rho}_2; c, \cdot} \text{CKTC\_OUT} \\
\frac{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1^s \Downarrow \widetilde{\rho}'_1, \widetilde{\rho}'_2; O_1 \quad \widetilde{\rho}'_1, \widetilde{\rho}'_2 \vdash \kappa_2^s \Downarrow \widetilde{\rho}''_1, \widetilde{\rho}''_2; O_2}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1^s, \kappa_2^s \Downarrow \widetilde{\rho}''_1, \widetilde{\rho}''_2; O_1, O_2} \text{CKTC\_SEQ}
\end{array}$$

Figure 14: Circuit command evaluation

$$\boxed{\psi \sim \tau}$$

$$\begin{array}{c}
\frac{}{\sigma \sim \sigma^\ell} \text{ST\_BT} \\
\frac{}{\sigma[n] \sim \sigma^\ell[n]} \text{ST\_ARR}
\end{array}$$

Figure 15: Source type and target type consistency

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

$$\begin{array}{c}
\overline{\Gamma \vdash \cdot \hookrightarrow \cdot; \cdot, \cdot} \quad \text{EN\_EMP} \\
\\
\begin{array}{c}
\Gamma(x) = \sigma^{\mathcal{P}} \\
c : \sigma \\
\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2
\end{array} \\
\hline
\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \tilde{\rho}[x \mapsto c]; \hat{\rho}_1, \hat{\rho}_2 \quad \text{EN\_PBT} \\
\\
\begin{array}{c}
\Gamma(x) = \sigma^m \\
c : \sigma \\
r = \text{next\_range}() \\
(b_1, b_2) = \mathcal{E}_m(c) \\
\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2
\end{array} \\
\hline
\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \tilde{\rho}[x \mapsto r]; \hat{\rho}_1[r \mapsto b_1], \hat{\rho}_2[r \mapsto b_2] \quad \text{EN\_SBT} \\
\\
\begin{array}{c}
\Gamma(x) = \sigma^{\mathcal{P}}[n] \\
\forall i \in \{0, n-1\}. c_i : \sigma \\
\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2
\end{array} \\
\hline
\Gamma \vdash \rho[x \mapsto [c_i]_n] \hookrightarrow \tilde{\rho}[x \mapsto [c_i]_n]; \hat{\rho}_1, \hat{\rho}_2 \quad \text{EN\_PARR} \\
\\
\begin{array}{c}
\Gamma(x) = \sigma^m[n] \\
\forall i \in \{0, n-1\}. (c_i : \sigma \wedge (r_i = \text{next\_range}() \wedge (b_{1\ i}, b_{2\ i}) = \mathcal{E}_m(c_i))) \\
\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2
\end{array} \\
\hline
\Gamma \vdash \rho[x \mapsto [c_i]_n] \hookrightarrow \tilde{\rho}[x \mapsto [r_i]_n]; \hat{\rho}_1[r_i \mapsto b_{1\ i}], \hat{\rho}_2[r_i \mapsto b_{2\ i}] \quad \text{EN\_SARR}
\end{array}$$

Figure 16: Source environment to target environment compilation