| | | | |
|---|---|---|---|
| $\sigma$ | ::= | | Base type |
| | $\mid$ | $\mathsf{uint}$ | |
| | $\mid$ | $\mathsf{bool}$ | |
| $\psi$ | ::= | | Source type |
| | $\mid$ | $\sigma$ | |
| | $\mid$ | $\sigma[n]$ | |
| $c$ | ::= | | Constant |
| | $\mid$ | $n$ | |
| | $\mid$ | $\top$ | |
| | $\mid$ | $\bot$ | |
| $e$ | ::= | | Source expression |
| | $\mid$ | $c$ | |
| | $\mid$ | $x$ | |
| | $\mid$ | $e_1 + e_2$ | |
| | $\mid$ | $\mathbf{cond}(e, e_1, e_2)$ | |
| | $\mid$ | $e_1 > e_2$ | |
| | $\mid$ | $[e_i]_n$ | |
| | $\mid$ | $x[e]$ | |
| | $\mid$ | $\mathbf{in}_j$ | |
| $s$ | ::= | | Source statement |
| | $\mid$ | $\psi\, x = e$ | |
| | $\mid$ | $x := e$ | |
| | $\mid$ | $\mathbf{for}\ x\ \mathbf{in}\ n_1 \ldots n_2\ \mathbf{do}\ s$ | |
| | $\mid$ | $x[e_1] := e_2$ | |
| | $\mid$ | $\mathbf{if}(e, s_1, s_2)$ | |
| | $\mid$ | $\mathbf{out}\, e$ | |
| | $\mid$ | $s_1; s_2$ | |

Figure 1: Source language

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

Figure 2: Source runtime

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

$$\frac{}{\rho \vdash c \Downarrow c} \text{ SE\_CONST}$$

$$\frac{}{\rho \vdash x \Downarrow \rho(x)} \text{ SE\_VAR}$$

$$\frac{\forall i \in \{1,2\}.\ \rho \vdash e_i \Downarrow n_i}{\rho \vdash e_1 + e_2 \Downarrow n_1 + n_2} \text{ SE\_ADD}$$

$$\frac{\begin{array}{l}\rho \vdash e \Downarrow c \\ c = \top \Rightarrow i = 1 \\ c = \bot \Rightarrow i = 2 \\ \rho \vdash e_i \Downarrow v\end{array}}{\rho \vdash \mathbf{cond}(e, e_1, e_2) \Downarrow v} \text{ SE\_COND}$$

$$\frac{\forall i \in \{1,2\}.\ \rho \vdash e_i \Downarrow n_i}{\rho \vdash e_1 > e_2 \Downarrow n_1 > n_2} \text{ SE\_GT}$$

$$\frac{\forall i \in \{0, n-1\}.\ \rho \vdash e_i \Downarrow c_i}{\rho \vdash [e_i]_n \Downarrow [c_i]_n} \text{ SE\_ARR}$$

$$\frac{\begin{array}{l}\rho \vdash x \Downarrow [c_i]_{n'} \\ \rho \vdash e \Downarrow n \\ n < n'\end{array}}{\rho \vdash x[e] \Downarrow c_n} \text{ SE\_AREAD}$$

$$\frac{}{\rho \vdash \mathbf{in}_j \Downarrow c} \text{ SE\_INP}$$

Figure 3: Source expression evaluation

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

$$\frac{\rho \vdash e \Downarrow v}{\rho \vdash \psi\, x = e \Downarrow \rho[x \mapsto v]; \cdot} \quad \text{SC\_DECL}$$

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

$$\frac{\rho[x \mapsto n_1] \vdash \textbf{loop}\ x\ \textbf{until}\ n_2\ \textbf{do}\ s \Downarrow \rho_1; O}{\rho \vdash \textbf{for}\ x\ \textbf{in}\ n_1 \ldots n_2\ \textbf{do}\ s \Downarrow \rho_1 \setminus x; O} \quad \text{SC\_FORT}$$

$$\frac{\rho(x) > n_2}{\rho \vdash \textbf{loop}\ x\ \textbf{until}\ n_2\ \textbf{do}\ s \Downarrow \rho; O} \quad \text{SC\_LOOPT}$$

$$\frac{\begin{array}{l}\rho(x) \leq n_2 \\ \rho \vdash s \Downarrow \rho_1; O_1 \\ ([\rho_1]_{\mathsf{dom}(\rho)})[x \mapsto \rho(x) + 1] \vdash \textbf{loop}\ x\ \textbf{until}\ n_2\ \textbf{do}\ s \Downarrow \rho_2; O_2\end{array}}{\rho \vdash \textbf{loop}\ x\ \textbf{until}\ n_2\ \textbf{do}\ s \Downarrow \rho_2; O_1, O_2} \quad \text{SC\_LOOPI}$$

$$\frac{\begin{array}{c}\rho \vdash x \Downarrow [c_i]_{n'} \\ \rho \vdash e_1 \Downarrow n \\ \rho \vdash e_2 \Downarrow c \\ n < n'\end{array}}{\rho \vdash x[e_1] := e_2 \Downarrow \rho[x \mapsto [c_i]_{n'}[n \mapsto c]]; \cdot} \quad \text{SC\_AWRITE}$$

$$\frac{\begin{array}{c}\rho \vdash e \Downarrow c \\ c = \top \Rightarrow i = 1 \\ c = \bot \Rightarrow i = 2 \\ \rho \vdash s_i \Downarrow \rho'; O\end{array}}{\rho \vdash \textbf{if}(e, s_1, s_2) \Downarrow \rho'; O} \quad \text{SC\_IF}$$

$$\frac{\rho \vdash e \Downarrow c}{\rho \vdash \textbf{out}\, e \Downarrow \rho; c, \cdot} \quad \text{SC\_OUT}$$

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

Figure 4: Source command evaluation

$\boxed{v : \psi}$

$$\frac{}{c : \mathsf{typeof}(c)} \quad \text{V\_CONS}$$

$$\frac{\forall i \in \{0, n-1\}.\ c_i : \sigma}{[c_i]_n : \sigma[n]} \quad \text{V\_ARR}$$

Figure 5: Value typing

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

Figure 6: Target language

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

$$\frac{}{\Gamma \vdash c : \mathsf{typeof}(c)^{\mathcal{P}} \rightsquigarrow c} \quad \text{S\_CONS}$$

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

$$\frac{\begin{array}{l}\forall i \in \{1,2\}.\ \Gamma \vdash e_i : \mathsf{uint}^{\ell} \rightsquigarrow \widetilde{e}_i \\ \ell = \mathcal{P} \vee \ell = \mathcal{A}\end{array}}{\Gamma \vdash e_1 + e_2 : \mathsf{uint}^{\ell} \rightsquigarrow \widetilde{e}_1 +_{\ell} \widetilde{e}_2} \quad \text{S\_ADD}$$

$$\frac{\begin{array}{l}\Gamma \vdash e : \mathsf{bool}^{\ell} \rightsquigarrow \widetilde{e} \\ \forall i \in \{1,2\}.\ \Gamma \vdash e_i : \sigma^{\ell'} \rightsquigarrow \widetilde{e}_i \\ \ell = \mathcal{P} \vee (\ell = \mathcal{B} \wedge \ell' = \mathcal{B})\end{array}}{\Gamma \vdash \mathbf{cond}(e, e_1, e_2) : \sigma^{\ell'} \rightsquigarrow \mathbf{cond}_{\ell}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2)} \quad \text{S\_COND}$$

$$\frac{\begin{array}{l}\forall i \in \{1,2\}.\ \Gamma \vdash e_i : \mathsf{uint}^{\ell} \rightsquigarrow \widetilde{e}_i \\ \ell = \mathcal{P} \vee \ell = \mathcal{B}\end{array}}{\Gamma \vdash e_1 > e_2 : \mathsf{bool}^{\ell} \rightsquigarrow \widetilde{e}_1 >_{\ell} \widetilde{e}_2} \quad \text{S\_GT}$$

$$\frac{\forall i \in \{0, n-1\}.\ \Gamma \vdash e_i : \sigma^{\ell} \rightsquigarrow \widetilde{e}_i}{\Gamma \vdash [e_i]_n : \sigma^{\ell}[n] \rightsquigarrow [\widetilde{e}_i]_n} \quad \text{S\_ARR}$$

$$\frac{\begin{array}{l}\Gamma \vdash x : \sigma^{\ell}[n] \rightsquigarrow x \\ \Gamma \vdash e : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow \widetilde{e} \\ \Gamma \models e < n\end{array}}{\Gamma \vdash x[e] : \sigma^{\ell} \rightsquigarrow x[\widetilde{e}]} \quad \text{S\_AREAD}$$

$$\frac{}{\Gamma \vdash \mathbf{in}_j : \sigma^m \rightsquigarrow \mathbf{in}_j^m} \quad \text{S\_INP}$$

$$\frac{\Gamma \vdash e : \sigma^{\ell} \rightsquigarrow \widetilde{e}}{\Gamma \vdash e : \sigma^m \rightsquigarrow \widetilde{e} \rhd m} \quad \text{S\_SUB}$$

Figure 7: Expression compilation

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

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

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

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

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

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

$$\frac{\Gamma \vdash e : \sigma^{m} \rightsquigarrow \widetilde{e}}{\Gamma \vdash \mathbf{out}\, e \rightsquigarrow \mathbf{out}\, \widetilde{e} \mid \Gamma} \quad \text{C\_OUT}$$

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

Figure 8: Command compilation

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

Figure 9: Target runtime

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

$$\frac{}{\widetilde{\rho} \vdash c \mathrel{\tilde{\Downarrow}} c} \text{ EE\_CONST}$$

$$\frac{}{\widetilde{\rho} \vdash x \mathrel{\tilde{\Downarrow}} \widetilde{\rho}(x)} \text{ EE\_VAR}$$

$$\frac{\forall i \in \{1,2\}.\ \widetilde{\rho} \vdash \widetilde{e}_i \mathrel{\tilde{\Downarrow}} n_i}{\widetilde{\rho} \vdash \widetilde{e}_1 +_{\mathcal{P}} \widetilde{e}_2 \mathrel{\tilde{\Downarrow}} n_1 + n_2} \text{ EE\_PADD}$$

$$\frac{\forall i \in \{1,2\}.\ \widetilde{\rho} \vdash \widetilde{e}_i \mathrel{\tilde{\Downarrow}} \kappa^e_i}{\widetilde{\rho} \vdash \widetilde{e}_1 +_{\mathcal{A}} \widetilde{e}_2 \mathrel{\tilde{\Downarrow}} \mathsf{Add}(\kappa^e_1, \kappa^e_2)} \text{ EE\_SADD}$$

$$\frac{\begin{array}{l}\widetilde{\rho} \vdash \widetilde{e} \mathrel{\tilde{\Downarrow}} c \\ c = \top \Rightarrow i = 1 \\ c = \bot \Rightarrow i = 2 \\ \widetilde{\rho} \vdash \widetilde{e}_i \mathrel{\tilde{\Downarrow}} \widetilde{v}\end{array}}{\widetilde{\rho} \vdash \mathbf{cond}_{\mathcal{P}}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2) \mathrel{\tilde{\Downarrow}} \widetilde{v}} \text{ EE\_PCOND}$$

$$\frac{\begin{array}{l}\widetilde{\rho} \vdash \widetilde{e} \mathrel{\tilde{\Downarrow}} \kappa^e \\ \forall i \in \{1,2\}.\ \widetilde{\rho} \vdash \widetilde{e}_i \mathrel{\tilde{\Downarrow}} \kappa^e_i\end{array}}{\widetilde{\rho} \vdash \mathbf{cond}_{\mathcal{B}}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2) \mathrel{\tilde{\Downarrow}} \mathsf{Mux}(\kappa^e, \kappa^e_1, \kappa^e_2)} \text{ EE\_SCOND}$$

$$\frac{\forall i \in \{1,2\}.\ \widetilde{\rho} \vdash \widetilde{e}_i \mathrel{\tilde{\Downarrow}} n_i}{\widetilde{\rho} \vdash \widetilde{e}_1 >_{\mathcal{P}} \widetilde{e}_2 \mathrel{\tilde{\Downarrow}} n_1 > n_2} \text{ EE\_PGT}$$

$$\frac{\forall i \in \{1,2\}.\ \widetilde{\rho} \vdash \widetilde{e}_i \mathrel{\tilde{\Downarrow}} \kappa^e_i}{\widetilde{\rho} \vdash \widetilde{e}_1 >_{\mathcal{B}} \widetilde{e}_2 \mathrel{\tilde{\Downarrow}} \mathsf{Gt}(\kappa^e_1, \kappa^e_2)} \text{ EE\_SGT}$$

$$\frac{\widetilde{\rho} \vdash \widetilde{e}_i \mathrel{\tilde{\Downarrow}} \widetilde{w}_i}{\widetilde{\rho} \vdash [\widetilde{e}_i]_n \mathrel{\tilde{\Downarrow}} [\widetilde{w}_i]_n} \text{ EE\_ARR}$$

$$\frac{\begin{array}{l}\widetilde{\rho} \vdash \widetilde{e} \mathrel{\tilde{\Downarrow}} n \\ \widetilde{\rho} \vdash x \mathrel{\tilde{\Downarrow}} [\widetilde{w}_i]_{n'} \\ n < n'\end{array}}{\widetilde{\rho} \vdash x[\widetilde{e}] \mathrel{\tilde{\Downarrow}} \widetilde{w}_n} \text{ EE\_AREAD}$$

$$\frac{}{\widetilde{\rho} \vdash \mathbf{in}^m_j \mathrel{\tilde{\Downarrow}} \mathsf{In}^m_j} \text{ EE\_INP}$$

$$\frac{\widetilde{\rho} \vdash \widetilde{e} \mathrel{\tilde{\Downarrow}} \widetilde{w}}{\widetilde{\rho} \vdash \widetilde{e} \rhd m \mathrel{\tilde{\Downarrow}} \widetilde{w} \rhd m} \text{ EE\_COERCE}$$

Figure 10: Target expression evaluation

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

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

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

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

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

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

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

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

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

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

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

Figure 11: Target command evaluation

$$
\begin{array}{lll}
b & ::= & \text{Share (byte string)} \\
\widehat{\rho} & ::= & \text{Circuit environment} \\
& | & \cdot \\
& | & \widehat{\rho}[r \mapsto b]
\end{array}
$$

Figure 12: Circuit runtime

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

$$\frac{}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash r \Downarrow \widehat{\rho}_1[r], \widehat{\rho}_2[r]} \quad \text{CKTE\_R}$$

$$\frac{(b_1, b_2) = \mathcal{E}_m(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{In}_j^m \Downarrow b_1, b_2} \quad \text{CKTE\_IN}$$

$$\frac{\begin{array}{l}\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1^e \Downarrow b_{11}, b_{21} \\ \widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_2^e \Downarrow b_{12}, b_{22} \\ n_1 = \mathcal{D}_{\mathcal{A}}(b_{11}, b_{21}) \\ n_2 = \mathcal{D}_{\mathcal{A}}(b_{12}, b_{22}) \\ (b_1, b_2) = \mathcal{E}_{\mathcal{A}}(n_1 + n_2)\end{array}}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Add}(\kappa_1^e, \kappa_2^e) \Downarrow b_1, b_2} \quad \text{CKTE\_ADD}$$

$$\frac{\begin{array}{l}\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1^e \Downarrow b_{11}, b_{21} \\ \widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_2^e \Downarrow b_{12}, b_{22} \\ n_1 = \mathcal{D}_{\mathcal{B}}(b_{11}, b_{21}) \\ n_2 = \mathcal{D}_{\mathcal{B}}(b_{12}, b_{22}) \\ (b_1, b_2) = \mathcal{E}_{\mathcal{B}}(n_1 > n_2)\end{array}}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Gt}(\kappa_1^e, \kappa_2^e) \Downarrow b_1, b_2} \quad \text{CKTE\_GT}$$

$$\frac{\begin{array}{l}\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa^e \Downarrow b_1, b_2 \\ \widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1^e \Downarrow b_{11}, b_{21} \\ \widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_2^e \Downarrow b_{12}, b_{22} \\ c = \mathcal{D}_{\mathcal{B}}(b_1, b_2) \\ c_1 = \mathcal{D}_{\mathcal{B}}(b_{11}, b_{21}) \\ c_2 = \mathcal{D}_{\mathcal{B}}(b_{12}, b_{22}) \\ c = \top \Rightarrow (b_1', b_2') = \mathcal{E}_{\mathcal{B}}(c_1) \\ c = \bot \Rightarrow (b_1', b_2') = \mathcal{E}_{\mathcal{B}}(c_2)\end{array}}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Mux}(\kappa^e, \kappa_1^e, \kappa_2^e) \Downarrow b_1', b_2'} \quad \text{CKTE\_MUX}$$

$$\frac{(b_1, b_2) = \mathcal{E}_m(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash c \rhd m \Downarrow b_1, b_2} \quad \text{CKTE\_COERCEC}$$

$$\frac{\begin{array}{l}\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa^e \Downarrow b_1, b_2 \\ c = \mathcal{D}_{m_1}(b_1, b_2) \\ (b_1', b_2') = \mathcal{E}_m(c)\end{array}}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa^e \rhd m \Downarrow b_1', b_2'} \quad \text{CKTE\_COERCER}$$

Figure 13: Circuit expression evaluation

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

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

$$\frac{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa^e \Downarrow b_1, b_2}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Bind}(\kappa^e, r) \Downarrow \widehat{\rho}_1[r \mapsto b_1], \widehat{\rho}_2[r \mapsto b_1]; \cdot} \quad \text{CKTC\_BIND}$$

$$\frac{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa^e \Downarrow b_1, b_2 \quad c = \mathcal{D}_m(b_1, b_2)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Out}\ \kappa^e \Downarrow \widehat{\rho}_1, \widehat{\rho}_2; c, \cdot} \quad \text{CKTC\_OUT}$$

$$\frac{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1^s \Downarrow \widehat{\rho}'_1, \widehat{\rho}'_2; O_1 \quad \widehat{\rho}'_1, \widehat{\rho}'_2 \vdash \kappa_2^s \Downarrow \widehat{\rho}''_1, \widehat{\rho}''_2; O_2}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1^s, \kappa_2^s \Downarrow \widehat{\rho}''_1, \widehat{\rho}''_2; O_1, O_2} \quad \text{CKTC\_SEQ}$$

Figure 14: Circuit command evaluation

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

$$\frac{}{\sigma \sim \sigma^\ell} \quad \text{ST\_BT}$$

$$\frac{}{\sigma[n] \sim \sigma^\ell[n]} \quad \text{ST\_ARR}$$

Figure 15: Source type and target type consistency

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

$$\frac{}{\cdot \vdash \cdot \hookrightarrow \cdot; \cdot, \cdot} \quad \text{EN\_EMP}$$

$$\frac{\begin{array}{l}\Gamma(x) = \sigma^{\mathcal{P}} \\ \rho(x) = c \\ c : \sigma \\ \Gamma \setminus x \vdash \rho \setminus x \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2\end{array}}{\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}[x \mapsto c]; \widehat{\rho}_1, \widehat{\rho}_2} \quad \text{EN\_PBT}$$

$$\frac{\begin{array}{l}\Gamma(x) = \sigma^{m} \\ \rho(x) = c \\ c : \sigma \\ r = \mathsf{next\_range}() \\ (b_1, b_2) = \mathcal{E}_m(c) \\ \Gamma \setminus x \vdash \rho \setminus x \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2\end{array}}{\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}[x \mapsto r]; \widehat{\rho}_1[r \mapsto b_1], \widehat{\rho}_2[r \mapsto b_2]} \quad \text{EN\_SBT}$$

$$\frac{\begin{array}{l}\Gamma(x) = \sigma^{\mathcal{P}}[n] \\ \rho(x) = [c_i]_n \\ \forall i \in \{0, n-1\}.\ c_i : \sigma \\ \Gamma \setminus x \vdash \rho \setminus x \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2\end{array}}{\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}[x \mapsto [c_i]_n]; \widehat{\rho}_1, \widehat{\rho}_2} \quad \text{EN\_PARR}$$

$$\frac{\begin{array}{l}\Gamma(x) = \sigma^{m}[n] \\ \rho(x) = [c_i]_n \\ \forall i \in \{0, n-1\}.\ (c_i : \sigma \wedge (r_i = \mathsf{next\_range}() \wedge (b_{1\,i}, b_{2\,i}) = \mathcal{E}_m(c_i))) \\ \Gamma \setminus x \vdash \rho \setminus x \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2\end{array}}{\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}[x \mapsto [r_i]_n]; \widehat{\rho}_1[r_i \mapsto b_{1\,i}], \widehat{\rho}_2[r_i \mapsto b_{2\,i}]} \quad \text{EN\_SARR}$$

Figure 16: Source environment to target environment compilation