1 Formal Development

Correctness theorem that we will aim at:

If:

- $\Gamma \vdash s \rightsquigarrow \widetilde{s} \mid \Gamma'$
- $\Gamma \sim \rho$
- $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$
- $\rho \vdash s \downarrow \rho'; O$

Then:

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

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

Figure 1: Source language

$$
\begin{array}{lcll}
v & ::= & & \text{Source value} \\
 & | & c & \\
 & | & [c_i]_n & \\
\rho & ::= & & \text{Source runtime environment} \\
 & | & \cdot & \\
 & | & \rho[x \mapsto v] & \\
O & ::= & & \text{Source observation} \\
 & | & \cdot & \\
 & | & v, O &
\end{array}
$$

Figure 2: Source runtime

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

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

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

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

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

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

$$\frac{\begin{array}{l} \rho \vdash e \downarrow n_1 \\ \rho \vdash x \downarrow [c_i]_{n_2} \\ n_1 < n_2 \end{array}}{\rho \vdash x[e] \downarrow c_n} \quad \text{SE\_AREAD}$$

$$\frac{\begin{array}{l} \sigma = \mathsf{bool} \Rightarrow c = \top \vee c = \bot \\ \sigma = \mathsf{uint} \Rightarrow c = n \end{array}}{\rho \vdash \mathbf{input}_i^\sigma \downarrow c} \quad \text{SE\_INP}$$

Figure 3: Source expression evaluation

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

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

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

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

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

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

$$\frac{\begin{array}{l}\rho \vdash x \downarrow [c_i]_{n_2} \\ \rho \vdash e_1 \downarrow n_1 \\ \rho \vdash e_2 \downarrow c \\ n_1 < n_2\end{array}}{\rho \vdash x[e_1] := e_2 \downarrow \rho[x \mapsto [c_i]_{n_2}[n_1 \mapsto c]]; \cdot} \quad \text{SC\_AWRITE}$$

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

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

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

Figure 4: Source command evaluation

$\boxed{v : \psi}$

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

$$\frac{c_i : \sigma}{[c_i]_n : \sigma[n]} \quad \text{V\_ARR}$$

Figure 5: Value typing

$$
\begin{array}{lcll}
\widetilde{e} & ::= & & \text{Target expression} \\
 & | & c & \\
 & | & x & \\
 & | & \widetilde{e}_1 +_\ell \widetilde{e}_2 & \\
 & | & \mathbf{cond}_\ell(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2) & \\
 & | & \widetilde{e}_1 >_\ell \widetilde{e}_2 & \\
 & | & x[\widetilde{e}] & \\
 & | & \mathbf{input}_i^{(\sigma^m)} & \\
 & | & \widetilde{e} \triangleright m & \\
 & | & [\widetilde{e}_i]_n & \\
\widetilde{s} & ::= & & \text{Target statement} \\
 & | & \tau\, x = \widetilde{e} & \\
 & | & x := \widetilde{e} & \\
 & | & \mathbf{for}(x := n_1; x \leq n_2; x := x + 1)\ \widetilde{s} & \\
 & | & x[\widetilde{e}_1] := \widetilde{e}_2 & \\
 & | & \mathbf{if}(\widetilde{e}, \widetilde{s}_1, \widetilde{s}_2) & \\
 & | & \mathbf{out}\, \widetilde{e} & \\
 & | & \widetilde{s}_1; \widetilde{s}_2 & \\
\Gamma & ::= & & \text{Type environment} \\
 & | & \cdot & \\
 & | & \Gamma, x : \tau &
\end{array}
$$

Figure 6: Target language

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

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

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

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

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

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

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

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

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

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

$$\frac{}{\Gamma \vdash \mathbf{input}_i^{\sigma} : \sigma^m \rightsquigarrow \mathbf{input}_i^{(\sigma^m)}} \quad \text{S\_INP}$$

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

Figure 7: Expression compilation

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

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

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

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

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

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

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

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

Figure 8: Command compilation

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

Figure 9: Target runtime

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

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

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

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

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

$$\frac{\begin{array}{l}\widetilde{\rho} \vdash \widetilde{e} \Downarrow c; \kappa \\ c = \top \Rightarrow i = 1 \\ c = \bot \Rightarrow i = 2 \\ \widetilde{\rho} \vdash \widetilde{e}_i \Downarrow \widetilde{v}; \kappa_1\end{array}}{\widetilde{\rho} \vdash \mathbf{cond}_{\mathcal{P}}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2) \Downarrow \widetilde{v}; \kappa, \kappa_1} \quad \text{EE\_PCOND}$$

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

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

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

$$\frac{\begin{array}{l}\widetilde{\rho} \vdash \widetilde{e} \Downarrow n_1; \kappa_1 \\ \widetilde{\rho} \vdash x \Downarrow [\widetilde{w}_i]_{n_2}; \kappa_2 \\ n_1 < n_2\end{array}}{\widetilde{\rho} \vdash x[\widetilde{e}] \Downarrow \widetilde{w}_n; \kappa_1, \kappa_2} \quad \text{EE\_AREAD}$$

$$\frac{r = \mathsf{next\_range}()}{\widetilde{\rho} \vdash \mathbf{input}_i^{(\sigma^m)} \Downarrow r; \mathsf{Inp}_i \rhd_m r} \quad \text{EE\_INP}$$

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

$$\frac{\widetilde{\rho} \vdash \widetilde{e}_i \Downarrow \widetilde{w}_i; \kappa_i}{\widetilde{\rho} \vdash [\widetilde{e}_i]_n \Downarrow [\widetilde{w}_i]_n; \kappa_i} \quad \text{EE\_ARR}$$

Figure 10: Target expression evaluation

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

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

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

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

$$\frac{\widetilde{\rho}[x] > n_2}{\widetilde{\rho} \vdash \textbf{loop}\ x\ \textbf{until}\ n_2\ \{\widetilde{s}\} \Longrightarrow \widetilde{\rho}; \cdot} \quad \text{EC\_LOOPT}$$

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

$$\frac{\begin{array}{l} \widetilde{\rho} \vdash x \Downarrow [\widetilde{w}_i]_{n_2}; \cdot \\ \widetilde{\rho} \vdash \widetilde{e}_1 \Downarrow n_1; \kappa_1 \\ \widetilde{\rho} \vdash \widetilde{e}_2 \Downarrow \widetilde{w}; \kappa_2 \\ n_1 < n_2 \end{array}}{\widetilde{\rho} \vdash x[\widetilde{e}_1] := \widetilde{e}_2 \Longrightarrow \widetilde{\rho}[x \mapsto [\widetilde{w}_i]_{n_2}[n_1 \mapsto \widetilde{w}]]; \kappa_1, \kappa_2} \quad \text{EC\_AWRITE}$$

$$\frac{\begin{array}{l} \widetilde{\rho} \vdash \widetilde{e} \Downarrow c; \kappa_1 \\ c = \top \Rightarrow i = 1 \\ c = \bot \Rightarrow i = 2 \\ \widetilde{\rho} \vdash \widetilde{s}_i \Longrightarrow \widetilde{\rho}'; \kappa_2 \end{array}}{\widetilde{\rho} \vdash \textbf{if}(\widetilde{e}, \widetilde{s}_1, \widetilde{s}_2) \Longrightarrow \widetilde{\rho}'; \kappa_1, \kappa_2} \quad \text{EC\_IF}$$

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

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

Figure 11: Target command evaluation

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

Figure 12: Circuit runtime

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

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

$$\frac{\begin{array}{c} n_1 = \mathcal{D}_{\mathcal{A}}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1] \\ n_2 = \mathcal{D}_{\mathcal{A}}(\widehat{\rho}_1[r_2], \widehat{\rho}_2[r_2] \\ (b_1, b_2) = \mathcal{E}_{\mathcal{A}}(n_1 + n_2) \end{array}}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \oplus(r_1, r_2, r_3) \longmapsto \widehat{\rho}_1[r_3 \mapsto b_1], \widehat{\rho}_2[r_3 \mapsto b_2]; \cdot} \quad \text{CKT\_ADD}$$

$$\frac{\begin{array}{c} \top = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1] \\ c = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_2], \widehat{\rho}_2[r_2] \\ (b_1, b_2) = \mathcal{E}_{\mathcal{B}}(c) \end{array}}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Mux}(r_1, r_2, r_3, r_4) \longmapsto \widehat{\rho}_1[r_4 \mapsto b_1], \widehat{\rho}_2[r_4 \mapsto b_2]; \cdot} \quad \text{CKT\_MUXT}$$

$$\frac{\begin{array}{c} \bot = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1] \\ c = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_3], \widehat{\rho}_2[r_3] \\ (b_1, b_2) = \mathcal{E}_{\mathcal{B}}(c) \end{array}}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Mux}(r_1, r_2, r_3, r_4) \longmapsto \widehat{\rho}_1[r_4 \mapsto b_1], \widehat{\rho}_2[r_4 \mapsto b_2]; \cdot} \quad \text{CKT\_MUXF}$$

$$\frac{\begin{array}{c} n_1 = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1] \\ n_2 = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_2], \widehat{\rho}_2[r_2] \\ (b_1, b_2) = \mathcal{E}_{\mathcal{B}}(n_1 > n_2) \end{array}}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Gt}(r_1, r_2, r_3) \longmapsto \widehat{\rho}_1[r_3 \mapsto b_1], \widehat{\rho}_2[r_3 \mapsto b_2]; \cdot} \quad \text{CKT\_GT}$$

$$\frac{(b_1, b_2) = \mathcal{E}_m(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash c \rhd_m r_2 \longmapsto \widehat{\rho}_1[r_2 \mapsto b_1], \widehat{\rho}_2[r_2 \mapsto b_2]; \cdot} \quad \text{CKT\_COERCEC}$$

$$\frac{\begin{array}{c} c = \mathcal{D}_{m_1}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1] \\ (b_1, b_2) = \mathcal{E}_m(c) \end{array}}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash r_1 \rhd_m r_2 \longmapsto \widehat{\rho}_1[r_2 \mapsto b_1], \widehat{\rho}_2[r_2 \mapsto b_2]; \cdot} \quad \text{CKT\_COERCER}$$

$$\frac{(b_1, b_2) = \mathcal{E}_m(\mathsf{get\_input}(i))}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \mathsf{Inp}_i \rhd_m r \longmapsto \widehat{\rho}_1[r_2 \mapsto b_1], \widehat{\rho}_2[r_2 \mapsto b_2]; \cdot} \quad \text{CKT\_INP}$$

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

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

Figure 13: Circuit evaluation

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

$$\frac{}{\cdot \sim \cdot}\ \textsc{sen\_emp}$$

$$\frac{\begin{array}{c} v : \psi \\ \psi \sim \tau \\ \Gamma \sim \rho \end{array}}{\Gamma, x : \tau \sim \rho[x \mapsto v]}\ \textsc{sen\_bnd}$$

Figure 14: Source environment and type environment consistency

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

$$\frac{}{\Gamma \vdash \cdot \hookrightarrow \cdot; \cdot, \cdot}\ \textsc{en\_emp}$$

$$\frac{\begin{array}{c} \Gamma(x) = \sigma^{\mathcal{P}} \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2 \end{array}}{\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \widetilde{\rho}[x \mapsto c]; \widehat{\rho}_1, \widehat{\rho}_2}\ \textsc{en\_pbt}$$

$$\frac{\begin{array}{c} \Gamma(x) = \sigma^{m} \\ r = \mathsf{next\_range}() \\ (b_1, b_2) = \mathcal{E}_m(c) \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2 \end{array}}{\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \widetilde{\rho}[x \mapsto r]; \widehat{\rho}_1[r \mapsto b_1], \widehat{\rho}_2[r \mapsto b_2]}\ \textsc{en\_sbt}$$

$$\frac{\begin{array}{c} \Gamma(x) = \sigma^{\mathcal{P}}[n] \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2 \end{array}}{\Gamma \vdash \rho[x \mapsto [c_i]_n] \hookrightarrow \widetilde{\rho}[x \mapsto [c_i]_n]; \widehat{\rho}_1, \widehat{\rho}_2}\ \textsc{en\_parr}$$

$$\frac{\begin{array}{c} \Gamma(x) = \sigma^{m}[n] \\ r_i = \mathsf{next\_range}() \\ (b_{1\,i}, b_{2\,i}) = \mathcal{E}_m(c_i) \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2 \end{array}}{\Gamma \vdash \rho[x \mapsto [c_i]_n] \hookrightarrow \widetilde{\rho}[x \mapsto [r_i]_n]; \widehat{\rho}_1[r_i \mapsto b_{1\,i}], \widehat{\rho}_2[r_i \mapsto b_{2\,i}]}\ \textsc{en\_sarr}$$

Figure 15: Source environment to target environment compilation