1 Formal Development

Correctness theorem that we will aim at:

If:

- $\Gamma \vdash s \rightsquigarrow \widetilde{s} \mid \Gamma'$ (Compilation of source command)
- $\Gamma \sim \rho$ (Source environment, maps free variables to values)
- $\rho \vdash s \downarrow \rho'; O$ (Source semantics, no MPC)
- $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}$ (Compiling source environment to C++ environment, free secret variables are mapped to wire ranges)
- $\Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2$ (Compiling source enviroment to circuit environment, secret variables are converted to shares)

Then:

- $\widetilde{\rho} \vdash \widetilde{s} \Longrightarrow \widetilde{\rho}'; \kappa$ (The C++ ABY program)
- $\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa \longmapsto \widehat{\rho}'_1, \widehat{\rho}'_2; O$ (Circuit evaluation)

The setup is as follows: Programmer writes a source statement s. The statement s might have some free variables in it (i.e. variables that are used but not declared in the statement). For example, inputs of the two parties can be modeled this way, without having an explicit input command.

The initial type environment Γ gives types to the free variables of s. For example, say the parties inputs are x and y, and they are free in s, then $\Gamma = \cdot, x : \mathsf{uint}^{\mathcal{A}}, y : \mathsf{uint}^{\mathcal{A}}$.

The first premise compiles the statement s into a target statement $\widetilde{s}$ (the output type enviroment is not important for the top-most invocation of compilation). This judgment compiles operators into their public or secret versions, and inserts coercions (e.g. from $\mathcal{A}$ to $\mathcal{B}$).

Now we need to talk about evaluation. First, we have an ideal semantics for the source statements $\rho \vdash s \downarrow \rho'; O$. This ideal semantics effectively ignores the public/secret distinction, and just does plain evaluation, emitting observations for each $\mathbf{out}\,\widetilde{e}$ statement. In this judgment, ρ is the environment that maps free variables to values. The second premise says that the mappings in ρ are consistent with the mappings in Γ. For example, if a variable in Γ is boolean, then it indeed contains a boolean value in ρ (else our evaluation will get stuck). And the third judgment is the source evaluation (the ideal semantics).

The ideal semantics is realized in two steps. The first is where we only compute over public parts of the statement and generate a circuit. The judgment for this semantics is $\widetilde{\rho} \vdash \widetilde{s} \Longrightarrow \widetilde{\rho}'; \kappa$, where κ is the output circuit, and $\widetilde{\rho}$ is the environment (mapping from variables to values).

To start this evaluation, we need to correspond the $\widetilde{\rho}$ with ρ, i.e. somehow make sure that they are consistent. What is the notion of consistency here?

The consistency between ρ and $\widetilde{\rho}$ is defined as follows: For public variables, both should contain the same value, and for secret variables $\widetilde{\rho}$ should contain *a wire range*. That's essentially the fourth premise of the theorem. Γ in that premise helps us figure public/private annotations.

And then, the first conclusion of the theorem says that the C++ program evaluates well, and gives us a circuit. There are no observations in this phase.

Now what remains is evaluating the circuit κ generated in the first conclusion of the theorem.

The judgment $\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa \longmapsto \widehat{\rho}'_1, \widehat{\rho}'_2; O$ evaluates a circuit. In the circuit environment $\widehat{\rho}$, wire ranges are mapped to shares of values $\mathcal{E}_1^m(c)$ in $\widehat{\rho}_1$ and $\mathcal{E}_2^m(c)$ in $\widehat{\rho}_2$. The value $\mathcal{E}_1^m(c)$ is first m share of c, where m is $\mathcal{A}$ or $\mathcal{B}$.

But before we start evaluating the circuit, we have to make sure that the environments $\widehat{\rho}_1$ and $\widehat{\rho}_2$ are consistent with the source environment ρ. What is consistency here? For secret typed variables, we should split the mapping in ρ into shares and put them in $\widehat{\rho}_1$ and $\widehat{\rho}_2$, and ignore the public variables.

This is what the fifth premise does. And then the second conclusion says circuit evaluation generates same observations as in the source semantics.

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

Figure 1: Source language

$$
\begin{array}{lcll}
v & ::= & & \text{Source value} \\
 & | & c & \\
 & | & [\,\overline{c_i}^{\,i}\,] & \\
 & & & \\
\rho & ::= & & \text{Source runtime environment} \\
 & | & . & \\
 & | & \rho[x \mapsto v] & \\
 & & & \\
O & ::= & & \text{Source observation} \\
 & | & . & \\
 & | & v & \\
 & | & O_1, O_2 &
\end{array}
$$

Figure 2: Source runtime

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

$$\frac{}{\rho \vdash c \downarrow c}\ \textsc{se\_const}$$

$$\frac{}{\rho \vdash x \downarrow \rho(x)}\ \textsc{se\_var}$$

$$\frac{\rho \vdash e_i \downarrow n_i}{\rho \vdash e_1 + e_2 \downarrow n_1 + n_2}\ \textsc{se\_add}$$

$$\frac{\begin{array}{c}\rho \vdash e \downarrow \top \\ \rho \vdash e_1 \downarrow v\end{array}}{\rho \vdash \mathbf{cond}(e, e_1, e_2) \downarrow v}\ \textsc{se\_condt}$$

$$\frac{\begin{array}{c}\rho \vdash e \downarrow \bot \\ \rho \vdash e_2 \downarrow v\end{array}}{\rho \vdash \mathbf{cond}(e, e_1, e_2) \downarrow v}\ \textsc{se\_condf}$$

$$\frac{\rho \vdash e_i \downarrow n_i}{\rho \vdash e_1 > e_2 \downarrow n_1 > n_2}\ \textsc{se\_gt}$$

$$\frac{\begin{array}{l}\rho \vdash e \downarrow n \\ \rho \vdash x \downarrow [\,\overline{c_i}^{\,i}\,]\end{array}}{\rho \vdash x[e] \downarrow c_n}\ \textsc{se\_aread}$$

Figure 3: Source expression evaluation

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

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

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

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

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

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

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

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

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

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

Figure 4: Source command evaluation

$\boxed{v : \tau}$

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

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

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

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

Figure 5: Value typing

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

Figure 6: Target language

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

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

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

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

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

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

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

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

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

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

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

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

$$\frac{\begin{array}{l}\Gamma \vdash e : \sigma_1 \rightsquigarrow \widetilde{e} \\ \mathsf{base}(\sigma_1) = \mathsf{base}(\sigma_2) \\ \mathsf{label}(\sigma_2) = m\end{array}}{\Gamma \vdash e : \sigma_2 \rightsquigarrow \widetilde{e} \rhd m}\ \textsc{S\_SUB}$$

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

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

Figure 9: Target runtime

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

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

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

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

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

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

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

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

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

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

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

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

Figure 10: Target expression evaluation

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

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

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

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

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

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

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

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

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

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

Figure 11: Target command evaluation

$$
\begin{array}{llll}
\widehat{c} & ::= & & \text{Circuit value (share)} \\
 & \mid & \mathcal{E}_1^m(c) & \\
 & \mid & \mathcal{E}_2^m(c) & \\
 & & & \\
\widehat{\rho} & ::= & & \text{Circuit environment} \\
 & \mid & \cdot & \\
 & \mid & \widehat{\rho}[r \mapsto \widehat{c}] &
\end{array}
$$

Figure 12: Circuit runtime

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

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

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

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

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

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

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

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

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

Figure 13: Circuit evaluation

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

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

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

Figure 14: Source environment and type environment consistency

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

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

$$\frac{\begin{array}{l} \Gamma(x) = \sigma \\ \mathsf{label}(\sigma) = \mathcal{P} \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho} \end{array}}{\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \widetilde{\rho}[x \mapsto c]}\ \text{TEN\_PBT}$$

$$\frac{\begin{array}{l} \Gamma(x) = \sigma \\ \mathsf{label}(\sigma) = m \\ r = \mathsf{next\_range}() \\ \Gamma \vdash \rho \hookrightarrow \widetilde{\rho} \end{array}}{\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \widetilde{\rho}[x \mapsto r]}\ \text{TEN\_SBT}$$

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

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

Figure 15: Source environment to target environment compilation

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

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

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

$$\frac{\begin{array}{l} \Gamma(x) = \sigma \\ \mathsf{label}(\sigma) = m \\ \widetilde{\rho}[x] = r \\ \Gamma; \widetilde{\rho} \vdash \rho \hookrightarrow \widehat{\rho}_1, \widehat{\rho}_2 \end{array}}{\Gamma; \widetilde{\rho} \vdash \rho[x \mapsto c] \hookrightarrow \widehat{\rho}_1[r \mapsto \mathcal{E}_1^m(c)], \widehat{\rho}_2[r \mapsto \mathcal{E}_2^m(c)]} \quad \text{CEN\_SBT}$$

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

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

Figure 16: Source environment to circuit environment compilation