[Aseem: I am currently using same e syntax for source and target. Please understand as: the programmer always writes public versions of the operators, conditionals etc. Then our compiler translates some of them to secret operators, leaving some of them as public. Note in the typing rules, the source expression always has public subscript.]

[Aseem: Also, I am still using the i notation in the premises of the inference rules as a convenience for now.]

[Aseem: The new bit is the circuit part in the evaluation semantics. Expressions evaluate to a value, and emit a circuit. The circuits are stitched together with wires. r represents a range of wire ids that represent a source level value. A meta-function next_range() gives the next ids. It can be implemented using a counter, for example.]

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

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

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

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

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

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

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 +_{\mathcal{P}} e_2 : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_1' +_{\mathcal{P}} e_2'} \ \text{S\_PADD}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{A}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 +_{\mathcal{P}} e_2 : \mathsf{uint}^{\mathcal{A}} \rightsquigarrow e_1' +_{\mathcal{A}} e_2'} \ \text{S\_SADD}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 \times_{\mathcal{P}} e_2 : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_1' \times_{\mathcal{P}} e_2'} \ \text{S\_PMULT}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{A}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 \times_{\mathcal{P}} e_2 : \mathsf{uint}^{\mathcal{A}} \rightsquigarrow e_1' \times_{\mathcal{A}} e_2'} \ \text{S\_SMULT}$$

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

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

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 >_{\mathcal{P}} e_2 : \mathsf{bool}^{\mathcal{P}} \rightsquigarrow e_1' >_{\mathcal{P}} e_2'} \ \text{S\_PGT}$$

$$\frac{\Gamma \vdash e_i : \mathsf{uint}^{\mathcal{B}} \rightsquigarrow e_i'}{\Gamma \vdash e_1 >_{\mathcal{P}} e_2 : \mathsf{bool}^{\mathcal{B}} \rightsquigarrow e_1' >_{\mathcal{B}} e_2'} \ \text{S\_SGT}$$

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

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

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

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

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

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

$$\frac{\begin{array}{l}\Gamma \vdash x : \sigma[\,] \rightsquigarrow x \\ \Gamma \vdash e_1 : \mathsf{uint}^{\mathcal{P}} \rightsquigarrow e_1' \\ \Gamma \vdash e_2 : \sigma \rightsquigarrow e_2'\end{array}}{\Gamma \vdash x[e_1] := e_2 \rightsquigarrow x[e_1'] := e_2' \mid \Gamma} \quad \text{C\_AWRITE}$$

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

$$\frac{\Gamma \vdash e : \tau \rightsquigarrow e'}{\Gamma \vdash \mathbf{out}\ e \rightsquigarrow \mathbf{out}\ e' \mid \Gamma} \quad \text{C\_OUT}$$

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

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

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

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

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

$$\frac{\rho \vdash e_i \Downarrow n_i; \kappa_i}{\rho \vdash e_1 +_{\mathcal{P}} e_2 \Downarrow n_1 + n_2; \kappa_1, \kappa_2} \quad \text{EE\_PADD}$$

$$\frac{\begin{array}{c}\rho \vdash e_i \Downarrow r_i; \kappa_i \\ r_3 = \mathsf{next\_range}()\end{array}}{\rho \vdash e_1 +_{\mathcal{A}} e_2 \Downarrow r_3; \kappa_1, \kappa_2, \oplus(r_1, r_2, r_3)} \quad \text{EE\_SADD}$$

$$\frac{\rho \vdash e_i \Downarrow n_i; \kappa_i}{\rho \vdash e_1 \times_{\mathcal{P}} e_2 \Downarrow n_1 \times n_2; \kappa_1, \kappa_2} \quad \text{EE\_PMULT}$$

$$\frac{\begin{array}{c}\rho \vdash e_i \Downarrow r_i; \kappa_i \\ r_3 = \mathsf{next\_range}()\end{array}}{\rho \vdash e_1 \times_{\mathcal{A}} e_2 \Downarrow r_3; \kappa_1, \kappa_2, \otimes(r_1, r_2, r_3)} \quad \text{EE\_SMULT}$$

$$\frac{\begin{array}{c}\rho \vdash e \Downarrow \top; \kappa \\ \rho \vdash e_1 \Downarrow v; \kappa_1\end{array}}{\rho \vdash \mathbf{cond}_{\mathcal{P}}(e, e_1, e_2) \Downarrow v; \kappa, \kappa_1} \quad \text{EE\_PCONDT}$$

$$\frac{\begin{array}{c}\rho \vdash e \Downarrow \bot; \kappa \\ \rho \vdash e_2 \Downarrow v; \kappa_2\end{array}}{\rho \vdash \mathbf{cond}_{\mathcal{P}}(e, e_1, e_2) \Downarrow v; \kappa, \kappa_2} \quad \text{EE\_PCONDF}$$

$$\frac{\begin{array}{c}\rho \vdash e \Downarrow r; \kappa \\ \rho \vdash e_i \Downarrow r_i; \kappa_i \\ r_3 = \mathsf{next\_range}()\end{array}}{\rho \vdash \mathbf{cond}_{\mathcal{B}}(e, e_1, e_2) \Downarrow r_3; \kappa, \kappa_1, \kappa_2, \mathsf{Mux}(r, r_1, r_2, r_3)} \quad \text{EE\_SCOND}$$

$$\frac{\rho \vdash e_i \Downarrow n_i; \kappa_i}{\rho \vdash e_1 >_{\mathcal{P}} e_2 \Downarrow n_1 > n_2; \kappa_1, \kappa_2} \quad \text{EE\_PGT}$$

$$\frac{\begin{array}{c}\rho \vdash e_i \Downarrow r_i; \kappa_i \\ r_3 = \mathsf{next\_range}()\end{array}}{\rho \vdash e_1 >_{\mathcal{B}} e_2 \Downarrow r_3; \kappa_1, \kappa_2, \mathsf{Gt}(r_1, r_2, r_3)} \quad \text{EE\_SGT}$$

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

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

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

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

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

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

$$\frac{\begin{array}{l} n_2 \geq n_1 \\ \rho[x \mapsto n_1] \vdash s \Downarrow \rho_1; \kappa_1 \\ \rho_1 \vdash \mathbf{for}(x := n_1 + 1; x \leq n_2; x := x + 1)\ s \Downarrow \rho_2; \kappa_2 \end{array}}{\rho \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1)\ s \Downarrow \rho_2; \kappa_1, \kappa_2} \quad \text{EC\_FORI}$$

$$\frac{\begin{array}{l} \rho \vdash x \Downarrow [\,\overline{w_i}^{\,i}\,]; \cdot \\ \rho \vdash e_1 \Downarrow n; \kappa_1 \\ \rho \vdash e_2 \Downarrow w; \kappa_2 \end{array}}{\rho \vdash x[e_1] := e_2 \Downarrow \rho[x \mapsto [\,\overline{w_i}^{\,i}\,][n \mapsto w]]; \kappa_1, \kappa_2} \quad \text{EC\_AWRITE}$$

$$\frac{\begin{array}{c} \rho \vdash e \Downarrow \top; \kappa_1 \\ \rho \vdash s_1 \Downarrow \rho'; \kappa_2 \end{array}}{\rho \vdash \mathbf{if}(e, s_1, s_2) \Downarrow \rho'; \kappa_1, \kappa_2} \quad \text{EC\_IFT}$$

$$\frac{\begin{array}{c} \rho \vdash e \Downarrow \bot; \kappa_1 \\ \rho \vdash s_2 \Downarrow \rho'; \kappa_2 \end{array}}{\rho \vdash \mathbf{if}(e, s_1, s_2) \Downarrow \rho'; \kappa_1, \kappa_2} \quad \text{EC\_IFF}$$

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

$$\frac{\begin{array}{c} \rho \vdash s_1 \Downarrow \rho_1; \kappa_1 \\ \rho_1 \vdash s_2 \Downarrow \rho_2; \kappa_2 \end{array}}{\rho \vdash s_1; s_2 \Downarrow \rho_2; \kappa_1, \kappa_2} \quad \text{EC\_SEQ}$$