σ	::=		Base type
	$\mid$	uint	
	$\mid$	bool	
ψ	::=		Source type
	$\mid$	σ	
	$\mid$	$\sigma[n]$	
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	
	$\mid$	$[c_i]_n$	
ρ	::=		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
	$\mid$	$\mathcal{A}$	
	$\mid$	$\mathcal{B}$	
ℓ	$::=$		Label
	$\mid$	$\mathcal{P}$	
	$\mid$	m	
τ	$::=$		Type
	$\mid$	σ^{ℓ}	
	$\mid$	$\sigma^{\ell}[n]$	
$\widetilde{e}$	$::=$		Target expression
	$\mid$	c	
	$\mid$	x	
	$\mid$	$\widetilde{e}_1 +_{\ell} \widetilde{e}_2$	
	$\mid$	$\mathbf{cond}_{\ell}(\widetilde{e}, \widetilde{e}_1, \widetilde{e}_2)$	
	$\mid$	$\widetilde{e}_1 >_{\ell} \widetilde{e}_2$	
	$\mid$	$[\widetilde{e}_i]_n$	
	$\mid$	$x[\widetilde{e}]$	
	$\mid$	$\mathbf{input}_j^m$	
	$\mid$	$\widetilde{e} \rhd m$	
$\widetilde{s}$	$::=$		Target statement
	$\mid$	$\tau\, x = \widetilde{e}$	
	$\mid$	$x := \widetilde{e}$	
	$\mid$	$\mathbf{for}(x := n_1; x \leq n_2; x := x + 1)\ \widetilde{s}$	
	$\mid$	$x[\widetilde{e}_1] := \widetilde{e}_2$	
	$\mid$	$\mathbf{if}(\widetilde{e}, \widetilde{s}_1, \widetilde{s}_2)$	
	$\mid$	$\mathbf{out}\, \widetilde{e}$	
	$\mid$	$\widetilde{s}_1; \widetilde{s}_2$	
Γ	$::=$		Type environment
	$\mid$	$\cdot$	
	$\mid$	$\Gamma, x : \tau$	

Figure 6: Target language

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

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

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

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

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

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

Figure 7: Expression compilation

Figure 8: Command compilation

Figure 9: Target runtime

Figure 10: Target expression evaluation

Figure 11: Target command evaluation

Figure 12: Circuit runtime

Figure 13: Circuit evaluation

Figure 14: Source type and target type consistency

Figure 15: Source environment and type environment consistency

Figure 16: Source environment to target environment compilation