1 Formal Development

Lemma 1 (Value inversion)**.** *Inversion lemma for values:*

1. *If* $v : \mathsf{uint}$*, then* $v = n$

2. *If* $v : \mathsf{bool}$*, then* $v = \top$ *or* $v = \bot$

3. *If* $v : \sigma[n]$*, then* $v = [c_i]_n$ *and* $c_i : \sigma$

Lemma 2 (Consistency of source type and target type)**.** *If* $\psi \sim \tau$*, then one of the following holds:*

1. $\psi = \sigma$ *and* $\tau = \sigma^{\ell}$*.*

2. $\psi = \sigma[n]$ *and* $\tau = \sigma^{\ell}[n]$*.*

Lemma 3 (Compilation of source environment)**.** *If* $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$ *and* $\Gamma(x) = \tau$*, then one of the following holds:*

1. $\tau = \sigma^{\mathcal{P}}$*,* $\rho(x) = c$*,* $c : \sigma$*, and* $\widetilde{\rho}(x) = c$*.*

2. $\tau = \sigma^{m}$*,* $\rho(x) = c$*,* $c : \sigma$*,* $\widetilde{\rho}(x) = r$*, and* $(\widehat{\rho}_1[r], \widehat{\rho}_2[r]) = \mathcal{E}_m(c)$*.*

3. $\tau = \sigma^{\mathcal{P}}[n]$*,* $\rho(x) = [c_i]_n$*,* $\forall i \in \{0, n-1\}.\ c_i : \sigma$*, and* $\widetilde{\rho}(x) = [c_i]_n$*.*

4. $\tau = \sigma^{m}[n]$*,* $\rho(x) = [c_i]_n$*,* $\forall i \in \{0, n-1\}.\ c_i : \sigma$*,* $\widetilde{\rho}(x) = [r_i]_n$*,* $\forall i \in \{0, n-1\}.\ (\widehat{\rho}_1[r_i], \widehat{\rho}_2[r_i]) = \mathcal{E}_m(c_i)$

Lemma 4 (Soundness of public, scalar expressions)**.** *If*

1. $\Gamma \vdash e : \sigma^{\mathcal{P}} \rightsquigarrow \widetilde{e}$

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

Then

(a) $\rho \vdash e \Downarrow c$

(b) $c : \sigma$

(c) $\widetilde{\rho} \vdash \widetilde{e}\ \widetilde{\Downarrow}\ c$

Lemma 5 (Soundness of public, array expressions)**.** *If*

1. $\Gamma \vdash e : \sigma^{\mathcal{P}}[n] \rightsquigarrow \widetilde{e}$

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

Then

(a) $\rho \vdash e \Downarrow [c_i]_n$

(b) $\forall i \in \{0, n-1\}.\ c_i : \sigma$

(c) $\widetilde{\rho} \vdash \widetilde{e} \tilde{\Downarrow} [c_i]_n$

Lemma 6 (Soundness of secret, scalar expressions)**.** *If*

1. $\Gamma \vdash e : \sigma^m \rightsquigarrow \widetilde{e}$
2. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$

Then

(a) $\rho \vdash e \Downarrow c$

(b) $c : \sigma$

(c) $\widetilde{\rho} \vdash \widetilde{e} \tilde{\Downarrow} \kappa^e$

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

(e) $c = \mathcal{D}_m(b_1, b_2)$

Lemma 7 (Soundness of secret, array expressions)**.** *If*

1. $\Gamma \vdash e : \sigma^m[n] \rightsquigarrow \widetilde{e}$
2. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$

Then

(a) $\rho \vdash e \Downarrow [c_i]_n$

(b) $\forall i \in \{0, n-1\}.\ c_i : \sigma$

(c) $\widetilde{\rho} \vdash \widetilde{e} \tilde{\Downarrow} [\kappa^e_i]_n$

(d) $\forall i \in \{0, n-1\}.\ \widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa^e_i \Downarrow b_{1\,i}, b_{2\,i},\ s.t.\ c_i = \mathcal{D}_m(b_{1\,i}, b_{2\,i})$

Lemma 8 (Target semantics correspondence)**.** *If:*

1. $\Gamma \vdash s \rightsquigarrow \widetilde{s} \mid \Gamma'$
2. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$
3. $\rho \vdash s \Downarrow \rho'; O$

   then:

(a) $\widetilde{\rho} \vdash \widetilde{s} \tilde{\Downarrow} \widetilde{\rho}'; \kappa^s$

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

(c) $\Gamma' \vdash \rho' \hookrightarrow \widetilde{\rho}'; \widehat{\rho}'_1, \widehat{\rho}'_2$

Lemma 9 (Soundness of source semantics)**.** *If:*

1. $\Gamma \vdash s \rightsquigarrow \widetilde{s} \mid \Gamma'$

2. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$
3. *s is not a loop statement*

then:

(a) $\rho \vdash s \Downarrow \rho'; O$

(b) $\Gamma' \vdash \rho' \hookrightarrow \widetilde{\rho}'; \widehat{\rho}'_1, \widehat{\rho}'_2$

Lemma 10 (Termination of loop)**.** *If*

1. $\Gamma \vdash \textbf{loop } x \textbf{ until } n_2 \textbf{ do } s \rightsquigarrow \textbf{loop } x \textbf{ until } n_2 \textbf{ do } \widetilde{s} \mid \Gamma$
2. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$

then:

(a) $\rho \vdash \textbf{loop } x \textbf{ until } n_2 \textbf{ do } s \Downarrow \rho'; O$

(b) $\Gamma \vdash \rho' \hookrightarrow \widetilde{\rho}'; \widehat{\rho}'_1, \widehat{\rho}'_2$

Theorem 11 (Soundness)**.** *If:*

1. $\Gamma \vdash s \rightsquigarrow \widetilde{s} \mid \Gamma'$
2. $\Gamma \vdash \rho \hookrightarrow \widetilde{\rho}; \widehat{\rho}_1, \widehat{\rho}_2$

then:

(a) $\rho \vdash s \Downarrow \rho'; O$

(b) $\widetilde{\rho} \vdash \widetilde{s} \,\widetilde{\Downarrow}\, \widetilde{\rho}'; \kappa^s$

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

(d) $\Gamma' \vdash \rho' \hookrightarrow \widetilde{\rho}'; \widehat{\rho}'_1, \widehat{\rho}'_2$