1 Language

1.1 AST

$$e := x \mid v \mid \mathsf{f\_un}(e) \mid \mathsf{f\_bin}(e, e) \mid \mathsf{let}\ x = e\ \mathsf{in}\ e$$

$$\tau := \mathsf{public} \mid \mathsf{secret}$$

1.2 Typing Rules

$$\frac{x : \tau \in \Gamma}{\Gamma \vdash x : \tau}\ (\text{T-}\textsc{Var}) \qquad \frac{}{\vdash v : \mathsf{public}}\ (\text{T-}\textsc{Val})$$

$$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \mathsf{f\_un}(e) : \tau}\ (\text{T-}\textsc{UnFun}) \qquad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash \mathsf{f\_bin}(e_1, e_2) : \mathsf{max}(\tau_1, \tau_2)}\ (\text{T-}\textsc{BinFun})$$

$$\frac{\Gamma \vdash e_1 : \tau_1 \quad \Gamma, x : \tau_1 \vdash e_2 : \tau_2}{\Gamma \vdash \mathsf{let}\ x = e_1\ \mathsf{in}\ e_2 : \tau_2}\ (\text{T-}\textsc{Let})$$

The max function is defined as follows:

$$\mathsf{max} : \tau \times \tau \to \tau = \begin{cases} \mathsf{secret} & \text{if } \tau_1 \text{ is } \mathsf{secret} \lor \tau_2 \text{ is } \mathsf{secret} \\ \mathsf{public} & \text{otherwise} \end{cases}$$

1.3 Semantics

$$\frac{}{v \Rightarrow v}\ (\textsc{Val})$$

$$\frac{e \Rightarrow v}{f_{un}(e) \Rightarrow [[f_{un}]](v)}\ (\textsc{UnFun}) \qquad \frac{e_1 \Rightarrow v_1 \quad e_2 \Rightarrow v_2}{f_{bin}(e_1, e_2) \Rightarrow [[f_{bin}(v_1, v_2)]]}\ (\textsc{BinFun})$$

$$\frac{e_1 \Rightarrow v_1 \quad e_2[x \mapsto v_1] \Rightarrow v_2}{\mathsf{let}\ x = e_1\ \mathsf{in}\ e_2 \Rightarrow v_2}\ (\textsc{Let})$$